# SONY

# EVERYTHING ELSE PALES IN CONTRAST

# BRAVIA
## OLED

True reality comes to life with deep black and natural colour. Over 8 million self-illuminating pixels are precisely and individually controlled by the Picture Processor X1™ Extreme processor. Sony's 4K OLED TV creates exquisite, unprecedented contrast.

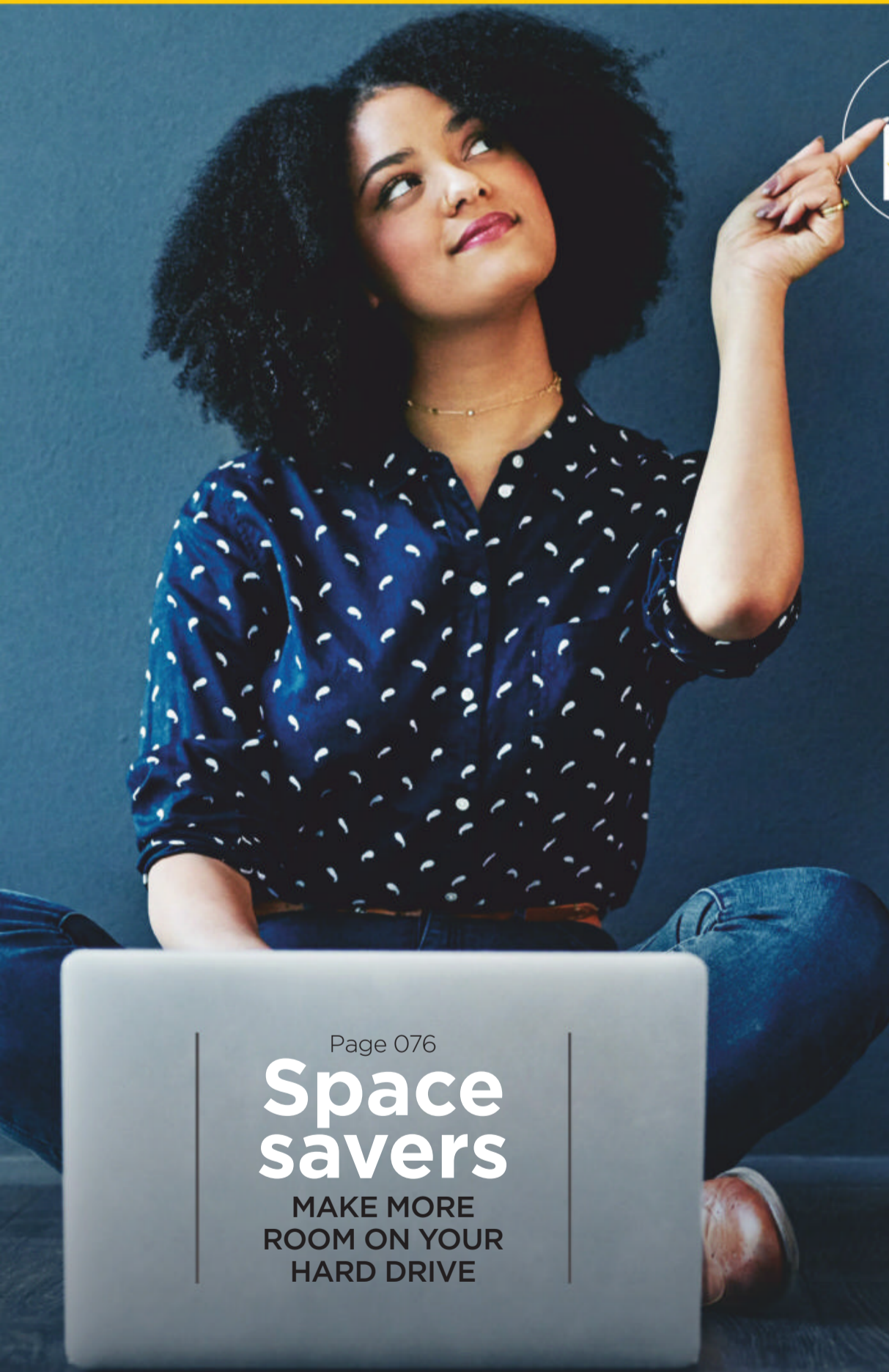Reviewed! Dell's new XPS 13 2-in-1 impresses

# TECH*life*

AUSTRALIA

Live life smarter

EXPERT GUIDE

# KEEP YOUR LAPTOP SECURE!

**SEEK & DESTROY MALWARE, CREATE PERFECT PASSWORDS, PROTECT YOUR DATA**

FUTURE

# DENON

# UPGRADE TO SUPERB WIRELESS SOUND.

**HEOS** BUILT-IN · WORKS WITH **alexa** · works with the **Google Assistant** · Works with **Apple AirPlay**

The Denon Home Wireless Speakers mark a new milestone in the development of best-in-class audio components, built on 110 years of audio excellence. Thanks to their Denon sound master tuning you can enjoy exceptional sound, seamlessly streamed from your favourite services via Wi-Fi, AirPlay2 or Bluetooth®, even in high resolution. With the HEOS Built-in technology you can group the speakers or connect them to Denon AV-receivers or sound bars.

## THE DENON HOME 150.
Pure class in a compact style, playing music with the great sound you'd expect from a Denon.

## THE DENON HOME 250.
This speaker impresses with an amazing sound stage taking your music into every corner.

## THE DENON HOME 350.
The flagship model of the family has the muscle to fill even large rooms with perfect sound.

## EXCELLENCE IN EVERY BEAT.
The Denon Home Wireless Speakers are built to deliver amazing audio quality. With their advanced acoustic hardware comprising high-class tweeters and woofers as well as class D power amplifiers they deliver excellence in every beat. Thanks to the built-in proximity sensor, the top display lights up as soon as you approach. Easily command the speaker by touch, e.g. store your favourite internet radio stations to enjoy them whenever you want, without the hassle of searching. Or you choose voice commands. With a smart speaker or your phone you can, depending on your region, use Amazon Alexa, Google Assistant and Apple Siri. The set-up? All done in minutes, just by using your mobile phone and the HEOS app.

## FEEL THE ENERGY OF A LIVE PERFORMANCE.
My Baby, an Amsterdam based band, is at home at big festival stages like Glastonbury or Lowlands. The three piece is full of praise for the expertly tuned Denon Home speakers. "*When it comes to sound, we're all very finicky.*" says Cato, the lead singer and guitar player. "*The Denon Home Wireless Speakers let the energy of a recording come across in your living room.*"

# UPGRADE TO DENON
**WWW.DENON.COM.AU**

# WELCOME

A few words from the boss…

# Tech in the time of COVID-19

I never thought I'd be opening a magazine by talking about the impact of a global pandemic – but here we are. And by "we", I mean a team of journalists now even more spread out than ever before, as we work remotely to try and do our bit to flatten the curve of COVID-19's spread.

In many ways everything is still business as usual; we want to bring you the latest news and reviews from the world of personal technology, and you're still as into it as we are. But, now, you might be even more interested, a little desperate for reading material as we try to limit our time outside. And while many of the world's big tech events are closing down – like the GDC and Mobile World Congress – the march of new releases remains relentless.

So, of course we have you covered. But alongside the reviews, this issue we also have a handy guide if, like us, you are now working from home. And, moving ahead in the coming months, we'll be aiming to help you find things to do from the seclusion of your own home, from hosting Netflix parties to where to watch the best sports without going near a stadium.

We are all in this together, and *TechLife* is here to help.

David Hollingworth, Editor

*Get in touch – tell me what you want to see more of in TechLife in the coming issues.*

# CONTENTS

Inside this issue of *TechLife*

# DOWNLOADS

Full-version commercial software exclusively for *TechLife* readers.

*"The built-in disc ripping auto-detects track names and easily turns audio files into custom audio discs.*

*"Abelssoft introduces a security program that can unmask and disable loggers before they obtain sensitive user data.*

## Burn baby, burn

Create stunning CDs, DVDs and Blu-Rays with Ashampoo Burning Studio 2020.
Full version worth $30

Ashampoo Burning Studio 2020 is a powerful disc burning software for CD, DVD and Blu-ray discs. The software quickly burns files, audio and video to all recordable disc types but also specialised media such as BDXL or M-Disc. The built-in disc ripping auto-detects track names and easily turns audio files into custom audio discs complete with individually designed covers and inlays. Playlists can be auto-generated during ripping for easy playback in the desired song order. The program can also finalise discs to make them playable on older retail players or car radios.
Download link: **www.ashampoo.com/techlifemagazine**

## Fend off online thieves

Neutralise spyware with Abelssoft AntiLogger.
Full version worth $50

"Loggers" are a variety of spyware that secretly install onto a PC and intercepts all keystrokes or taps on the user's screen. With AntiLogger, Abelssoft introduces a security program that can unmask and disable loggers before they obtain sensitive user data. Online crime is booming. And the favored tools of cyber-criminals are perfectly effective enough to provide them with plenty of valuable user data. Suspicious processes can easily be stopped with Abelssoft Antilogger, while benign processes falsely identified as malicious loggers will be placed on a "non-malicious software" list to prevent any further false alarms.
Download link: **www.techlife.net/exclusives**
Download ZIP password: **March20c**
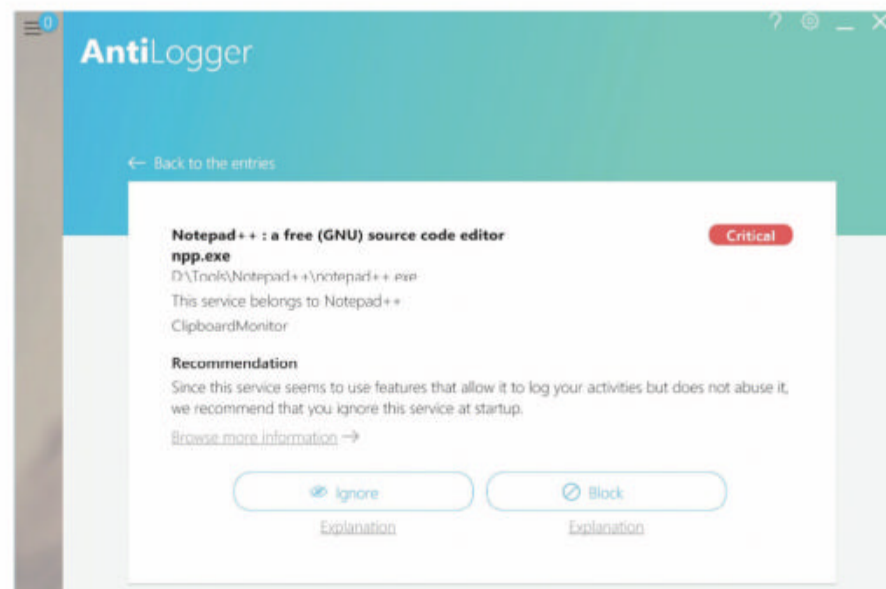
Please note that these exclusive downloads will only be available for a limited time, from **6/4/2020 to 24/5/2020**.

LEVEL UP

YOUR TV

au.yamaha.com

# YAMAHA
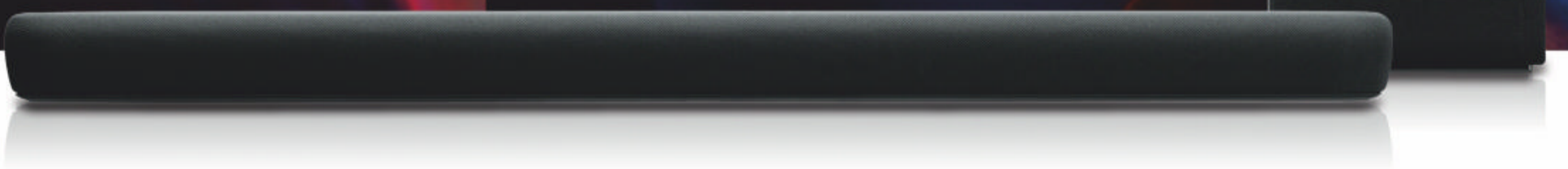
Enhance your TV, movie and gaming with built-in Alexa voice control, DTS® Virtual:X™ 3D surround sound, wireless subwoofer, and Bluetooth streaming all in a simple, sleek setup.

Introducing the new YAS-209 sound bar.

# HOTSPOT

$2,999, www.dell.com.au

## Dell XPS 13 2-in-1 (2019)

Giving the 13-inch MacBook Pro a run for its money.

You shouldn't judge a book by its cover, but by all means, go ahead and judge this one. Not that the Dell XPS 13 2-in-1 (2019) is a faultless machine, but it definitely has a lot going for it inside and out.

That unassuming yet high-quality Platinum Silver exterior, with its tiny 11.67 by 8.17-inch form factor and only the Dell symbol embossed in the middle, may make you curious enough about this laptop to pick it up. However, it's the endearing woven Arctic White interior (Black is also on offer) and ultraslim bezel FHD+ display that will get you hooked.

The first time we popped open the Dell XPS 13 2-in-1 (2019), we couldn't put it down. It doesn't just look good; it feels good as well beneath our hands. The keyboard has a matte finish that feels soft, while the textured woven areas on either side of the trackpad where your wrists rest actually feels nice and somehow

> **"**
> *It's the endearing woven Arctic White interior and ultraslim bezel FHD+ display that will get you hooked.*

helps keep your wrist from sliding.

Although having a white computer can be a tricky thing, since it's easier to see all the dirt and grime that pile up overtime, it doesn't feel like you need to be extra careful when using the Dell XPS 13 2-in-1 (2019). Simple regular cleaning should do it to keep the keyboard, trackpad and other areas clean, and that matte finish does keep

vibrant, impressively bright with 500 nits of brightness and has hardly any glare thanks to the 0.65% of anti-reflective coating.

Because it's made of Corning Gorilla Glass 5, the touchscreen also feels delightful beneath our fingertips. And, finally, those are the thinnest bezels we've ever seen, which not only gives you more screen real estate, but also gives that laptop a minimalist look.

## Performance

Armed with a 10th-generation Intel Core i7-1065G7 and coupled with 16GB of LPDDR4X memory, the Dell XPS 13 2-in-1 has more than enough power to deliver when tackling everyday computing tasks.

It's more than just a productivity laptop, though. While the Dell XPS 13 2-in-1 is only equipped with Intel Iris Plus graphics, this little laptop that could has proven that it's quite capable of handling casual gaming as well as light photo and video editing.

Obviously, this isn't a gaming computer by any means. It can, however, handle more casual and older games. We were able to run both *Civilization VI* and *Assassin's Creed Unity* on 1080p high, as well as *Vampyr*, a 2018 AAA game, without issue.

This isn't a video editing computer, either. However, we were curious about how it would handle it anyway. So, we made a minute and a half video on Adobe Premiere Pro using five stock clips. Rendering and exporting that video without added effects took about as long as the video itself: five and a half minutes with an effect added to each clip.

We had a bit of a rough start


The XPS 13's keyboard is supremely comfortable to use.

> ## "
> *Armed with a 10th-generation Intel Core i7-1065G7 and coupled with 16GB of LPDDR4X memory, the Dell XPS 13 2-in-1 has more than enough power to deliver when tackling everyday computing tasks.*

testing this laptop, as it couldn't "access graphics hardware" when we were trying to run the *Total War: Warhammer II* and *Shadow of the Tomb Raider*'s benchmarks. But, we did a refresh, ran CCleaner on the registry and for general computer issues, and updated both Dell and Windows drivers to find and fix the issues.

## Battery life

Whatever battery life a manufacturer is promising on a laptop usually ends up being longer than what you can actually expect, and that's also the case with the Dell XPS 13 2-in-1. Although Dell says that this laptop will last up to 16 hours, 58 minutes, it comes up considerably shorter during our tests.

In PCMark 8, which tests heavy productivity use, it makes it to 4 hours and 36 minutes (with 14% left on the battery). In the *TechRadar* battery test, where we loop 1080p video until the laptop dies, it lasts 7 hours and 50 minutes. Those results are pretty much on par with both the Lenovo Yoga C940 and HP Elite Dragonfly.

They're also far from the over 16 hours of longevity Dell has promised. However, that's good enough to get you through an entire day's work, given you're not pushing the laptop to its limits. But, just in case, we'd bring that charger.

★★★★☆

There's a lot to love about the Dell XPS 13 2-in-1 (2019), so much so that you'll be hard pressed to find fault in it. Beyond its stunning design, gorgeous display and portability, it also delivers enough power for productivity and even a bit of casual gaming.
Michelle Rae Uy

oil from your fingertips at bay.

Another feature worthy of praise here is the tiny HD webcam. Where the original had the camera below the display so that anyone you're chatting with ends up looking up at your nostrils, this 2019 model has it back in its rightful place. What's more is that Dell designed it to fit in the ultraslim top bezel, so what you get is a lens smaller than many other webcams out there but is just as capable of shooting at 720p resolution.

Speaking of the display, our review unit may only have the 13.4-inch display with 1920 x 1200 resolution – a 4K model is also available – but it's already plenty sharp for us. It's also incredibly

### NRL 2020: live stream this year's Rugby League season online

Kayo is a sports-centric streaming service, and for just AU$25 a month, you'll get access to over 50 sports live and on demand, which you can stream on up to two screens simultaneously. There's a 14-day free trial available for you to test out the service, and if you find it's not for you, you're free to cancel anytime as there are no lock-in contracts.

### Android 11 Developer Preview 2 promises improvements for foldable phones

Google launched its first Developer Preview of Android 11 much earlier than anticipated, and the tech giant has now followed it up with a second developer-focused (DP2) release of its mobile OS, building on some of the initial improvements and adding a few extras.

One of the main new additions found in DP2 is support for apps to communicate with the hinge sensors in foldable phones, allowing them to detect the angle that the phone is folded at and behave accordingly.

### Elon Musk says Tesla will make ventilators if supplies run low

Tesla CEO Elon Musk has said that his company has the ability to produce ventilators if US hospitals run into a shortage of breathing aids as a result of the ongoing coronavirus outbreak. When a Tesla owner reached out to Musk on Twitter asking him to repurpose the automaker's factories to make ventilators, he responded saying he would if there is a shortage.

# Apple's iPad Pro 2020 is said to be just '1% faster' than the 2018 version

Early benchmarks show minimal performance gains from A12Z chipset.

The iPad Pro 2020 boasts the souped-up A12Z Bionic chipset, though it turns out it's not much faster than the A12X Bionic chip at the heart of the iPad Pro 11 (2018) and iPad Pro 12.9 (2018), according to early benchmarks.

Specifically, the new iPad Pro is just 1% faster than the year-and-a-half old models that it's replacing, as per a listing on the benchmarking website *AnTuTu* and first spotted by *MySmartPrice*.

There's some good news, though, if you dive deeper into the benchmarks. We learn the baseline iPad Pro 2020 with 512GB of storage gets 6GB of RAM (previously, Apple stuck 4GB of RAM in all but the top-of-the-line 1TB version of the 2018 iPad Pro 12.9 model, which got 6GB).

We also see that the GPU speeds of the new iPad Pro are where Apple gives its new tablet some laptop-like oomph. That's likely to be good for 3D gaming apps and, in time, more advanced AR functionality to come.

Carly Page

# Google is halting all new Chrome updates

Remote workers need stable software, not new features.

As people all over the world are now working from home due to the ongoing coronavirus outbreak, Google has made the decision not to add any new features to both Chrome and Chrome OS in order to keep its software running as smoothly as possible.

In a tweet, the Chrome development team explained that it will pause upcoming Chrome and Chrome OS releases, saying:

"Due to adjusted work schedules, we're pausing upcoming Chrome & Chrome OS releases. Our goal is to ensure they continue to be stable, secure, & reliable for anyone who depends on them. We'll prioritise updates related to security, which will be included in Chrome 80. Stay tuned."

While updates often bring useful new features, they can also introduce new bugs into software which is why Google's decision to halt Chrome and Chrome OS updates makes a great deal of sense.

The Chrome development team also made the case that it's difficult to balance the browser's stability and new features while its employees are so decentralised.

Anthony Spadafora

# Five things you need to consider when working from home

Solid advice from industry professionals.

## Set and keep a routine

It's important to treat a workday at home very similar to a workday in the office. Have a schedule. Get up and get ready for work as you would if you were going into the office (although you don't need to dress up quite the same). Keep to standard 'office' hours. Minimise home chores to lunch breaks so as to not get distracted. And make sure you log off at a reasonable time. You may be able to squeeze in a bit more work without that commute, but keep it in check.

## Dedicated workspace

If you have a spare room you can use as your home office, that is great. But it doesn't need to be that elaborate. Set up an area of your home/apartment/room as your designated work space. Start each workday there. If you like to move around, you can do so as the day progresses and you get into the workflow, but oftentimes it's easier to get your day started when you are in a designated work area.

## Clear boundaries

Being home during your workday means it's easy for the lines between your work life and personal life to blur. Set specific guidelines and expectations for yourself and those around you. Discuss with your spouse, roommates, children exactly when you're available and when you're not and make sure that's clearly communicated at all times. On the flip side, be sure to know when to sign off and put your work away.

## Personal needs

Do you get stir crazy? Does 'watercooler' chat get you through the day? If you're craving that extra bit of stimulation, listen to yourself instead of pushing through it. Build yourself a 'work' playlist, schedule team check-ins and 1v1s, and let yourself step away during the day when you feel burnt out. Consider virtual team/co-worker lunches, with Zoom/Slack/Google Hangouts video conferencing on, to get some lighter social time in. The key here is listening to your own needs to make sure you don't burn out and can handle this system of working long term.

## Always communicate

Particularly for those of us used to working in office environments, the adjustment to working from home can be significant. If you work on a team or your work requires a great deal of collaboration, remember that (over) communication is key. This will save time and energy for all parties and make your entire team more efficient. If your team follows Agile practices, stick with your daily Standups and routines. Meet in the morning to go over what you did yesterday, what you are planning to do today, and any blockers you are facing. If you don't follow Agile, now is a good time to incorporate some elements into your routine to help improve your remote communication.

When you're working remotely, it's easy for time to become a sort of amorphous blob. But to actually be productive, it's essential to keep to a routine as much as possible. Setting a start time and an end time for your working day helps you to focus, adds structure, and ensures you don't get so lost in a task that you end up overworking and burning out.

**Dave Walters**, *Chief Technology Officer at Vettery, a data-driven, AI-powered hiring marketplace*
**Peter Coppinger**, *co-founder and CEO of Teamwork, a work management platform used by companies like Disney, Spotify and Netflix*
**Jean Hamon**, *CEO of community network Hivebrite.* **TL**

> *Set specific guidelines and expectations for yourself and those around you.*

$249, aftershokz.com

# Aftershokz Aeropex

The best bone conduction headphones you can buy.

Aftershokz has been in the running headphones game for a few years now, and in that time it's had one goal; to build open ear headphones you can run, cycle and and work out with, all without entirely blocking out the world around you.

It's gone all in on bone conduction technology built into an over the neck design to make that happen. With its latest, the Aeropex, it's managed to wrap that tech in something that's slimmer and more durable, all while adding new bone conduction tech to improve sound quality.

They're more expensive than its Trekz Air headphones, which launched back in 2017. For runners particularly, Aftershokz have fast become the go-to option as more races impose bans on the use of closed headphones and in-ear headphones due to safety concerns.

With very little competition in that sporty open ear headphones space, the Aeropex look to have cemented Aftershokz' place as the number one pick for fitness lovers once again.

## Design
With every new iteration, Aftershokz has successfully managed to shave a considerable amount of weight off the frame and the vital parts of its headphones, to make them lighter to wear and less noticeable when you're on the move. Put the Aeropex up

2020 TECHlife EDITOR'S CHOICE

alongside the Trekz Air and you can appreciate how much slimmer things have really gotten here.

Aftershokz says they're 30% smaller and 13% lighter, and while those sound like small numbers, the difference is very obvious as soon as you pick them up. These are considerably lighter than the last generation. It's still the same neckband-style look, but it's significantly reduced the size of the arms that sit just in front of your ears. The frame is skinnier too.

Things have been upped in the durability stakes moving from an IP55 water-resistant rating to a IP67 rating. That means you're getting something that's equipped to be submerged in water up to one meter depth for 30 minutes. In reality, that rating is about doing a better job of fending off sweat and increasing its chances of surviving for a run in the rain and maybe dropping them in a puddle on the way as opposed to taking them for a swim. Bluetooth and water don't mix anyway, so there'd be no reason to take them to the pool.

We did manage to brave a storm with them and get them sweaty for some indoor bike and rowing sessions and we are happy to report they've survived to live another day.

## Battery life
There's the promise of improved battery life here with the Aftershokz Aeropex. You're now getting eight hours of music playback and talk time, which is up two hours on the Airs. It also takes just one-and-a-half hours compared to two hours to fully charge up.

You're now also getting an hour of music playback from a quick 15-minute charge. When you first turn the headphones on and tap the buttons, it'll give you an status update on battery life to give you a heads up when it might be time for a spell on the charger.

If you're in the gym for an hour

a day or running for around the same amount of time, that's plenty of battery to play with for the week, and that's pretty much what we found.

## Audio quality
As we said, bone conduction technology remains at the heart of how Aftershokz delivers audio, in a way that doesn't entirely distract you from the world around you.

The way that bone conduction tech works hasn't changed for the Aeropex, using transducers to guide through vibrations up your cheek bones and to your ears, to deliver sound without needing to have something sitting directly inside of your ears.

What has changed is what Aftershokz refers to as 'PremiumPitch 2.0'. This time it's using the transducers to channel those vibrations that are angled to sit better on the cheekbone, promising to deliver sound that possesses more bass, less vibration and less sound leakage.

With the first generation of Aftershokz, those issues were very prominent. You didn't get a lot of power, they vibrated at higher volumes and they leaked a fair bit too. On the Aeropex, progress has certainly been made in some areas, but not in all. You are obviously not going

Sound is passed directly via bone conduction, which is pretty neat.

As with every release, the new headphones are lighter than previous models.

to get the kind of results you'd expect from an in ear or over-ear headphones, but there are some noticeable improvements with the very gentle upping of bass, improved detail and overall upgrade in audio quality.

Those improvements are more noticeable at moderate volume levels. Venture in the gym or for a run outside with them, and those improvements do shine through. Unlike previous models, there's a better balance between letting you hear the real world and letting your hear music or podcasts with more satisfying sound.

If you like breaking away from your workouts when a call comes through on your phone, there are dual, noise-cancelling mics to pick up your voice. You should have no problem taking those calls, though don't expect exceptional levels of clarity here.

★★★★☆

The Aftershokz Aeropex are the best bone conduction sports headphones you can buy right now. They are more expensive than previous models and deliver a noticeable, albeit slight jump up in sound quality. The slimmer design and improved battery life though are the reasons that will convince you it's worth spending a bit more.
Michael Sawh

# Bubbling vent discovered on Philippines seafloor

Newly discovered vent could be thousands of years old.

Diving hundreds of metres below the surface of the ocean off the coast of the Philippines, scientists came across a bubbling hotspot of carbon dioxide. And their research suggests that this newly discovered vent might help us predict how coral reefs will deal with climate change.

Bayani Cardenas, a professor in the department of geological sciences at the University of Texas at Austin, accidentally discovered this carbon dioxide fountain while researching the effect of groundwater run-off into the ocean environment in the Philippines's Verde Island Passage.

This strait that runs between the Luzon and Mindoro islands, connecting the South China Sea with the Tayabas Bay, is busy on its surface, serving as a prominent shipping route. It's also busy below the surface, where it harbours one of the most diverse marine ecosystems in the world. And the reefs in this passage, unlike bleached reefs elsewhere, are thriving.

The researchers named the new hotspot Soda Springs and said that it could have been releasing these bubbles for decades or even millennia. Soda Springs is a result of an underwater volcano, which vents gas and acidic water through cracks in the ocean floor. The researchers found carbon dioxide concentrations as high as 95,000 parts per million (ppm) near the springs, which is over 200 times the concentration present in the atmosphere.

The levels quickly fell as the gas flowed into the massive ocean, but the seafloor released enough gas to create elevated levels of 400 to 600 ppm and enough acidic water to lower the pH for the nearby coastline. This might be an ideal spot for studying how other coral reefs around the world may cope with climate change as it brings more carbon dioxide into their environments.

What's more, by tracing levels of radon-222, a naturally occurring radioactive isotope found in groundwater local to the area, the team discovered hotspots on the seafloor where groundwater was being discharged into the ocean. "Groundwater flow from land to sea could have important coastal impacts, but it is usually unrecognised," the authors wrote in the study. "Delicate reefs may be particularly sensitive to groundwater inputs."

The researchers found that groundwater and seawater appeared in different relative amounts in different areas of Soda Springs. This variable mixing means that "the groundwater flow could be contributing to the evolution and functioning of the ecosystem," the authors wrote.

However, the presence of these passageways might also mean that there is a way for pollutants from the island to make it into the coral reef. In the Philippines, where coastal development has surged, people are using septic tanks instead of modern sewage systems, which can easily pump waste into the reefs.

It's not clear how these reefs thrive in a carbon-dioxide-rich environment, but then again, not much is known about this area. "It's really a big part of the ocean that is left unexplored," Cardenes said. "It's too shallow for remotely operated vehicles and is too deep for regular divers."

A scientist collects gas samples at the newly discovered Soda Springs in the Philippines.
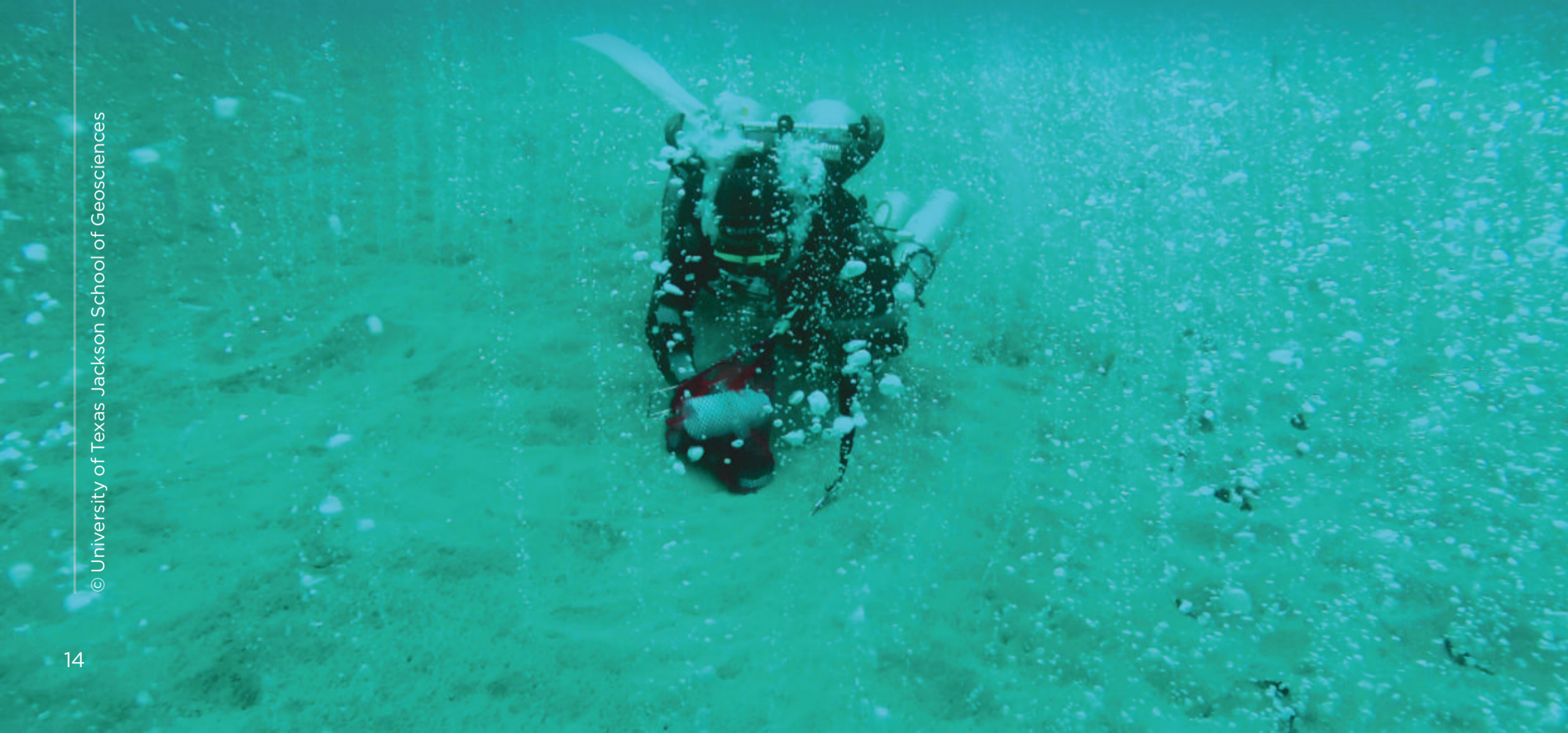
# Oldest meteorite crater found in Australia

Deep Aussie impact.

Despite Earth's long history of getting smacked by space rocks, evidence of those collisions can be very hard to find; even the largest impact craters vanish over time due to erosion and tectonic activity, taking the best reminders of Earth's past with them. Now, however, researchers in Western Australia believe they've found the single oldest impact crater ever detected, dating to roughly 2.2 billion years ago.

In a recent study, published in the journal Nature Communications, researchers studied a 70-kilometre impact site in the Australian Outback known as Yarrabubba. Today all that's visible of the once-enormous crater is a small red hill at the area's centre, known as Barlangi Hill. According to the researchers, the minerals inside that hill



Researchers drew the estimated shape of the Yarrabubba impact crater over this Google Earth image of Western Australia.

© Google Earth
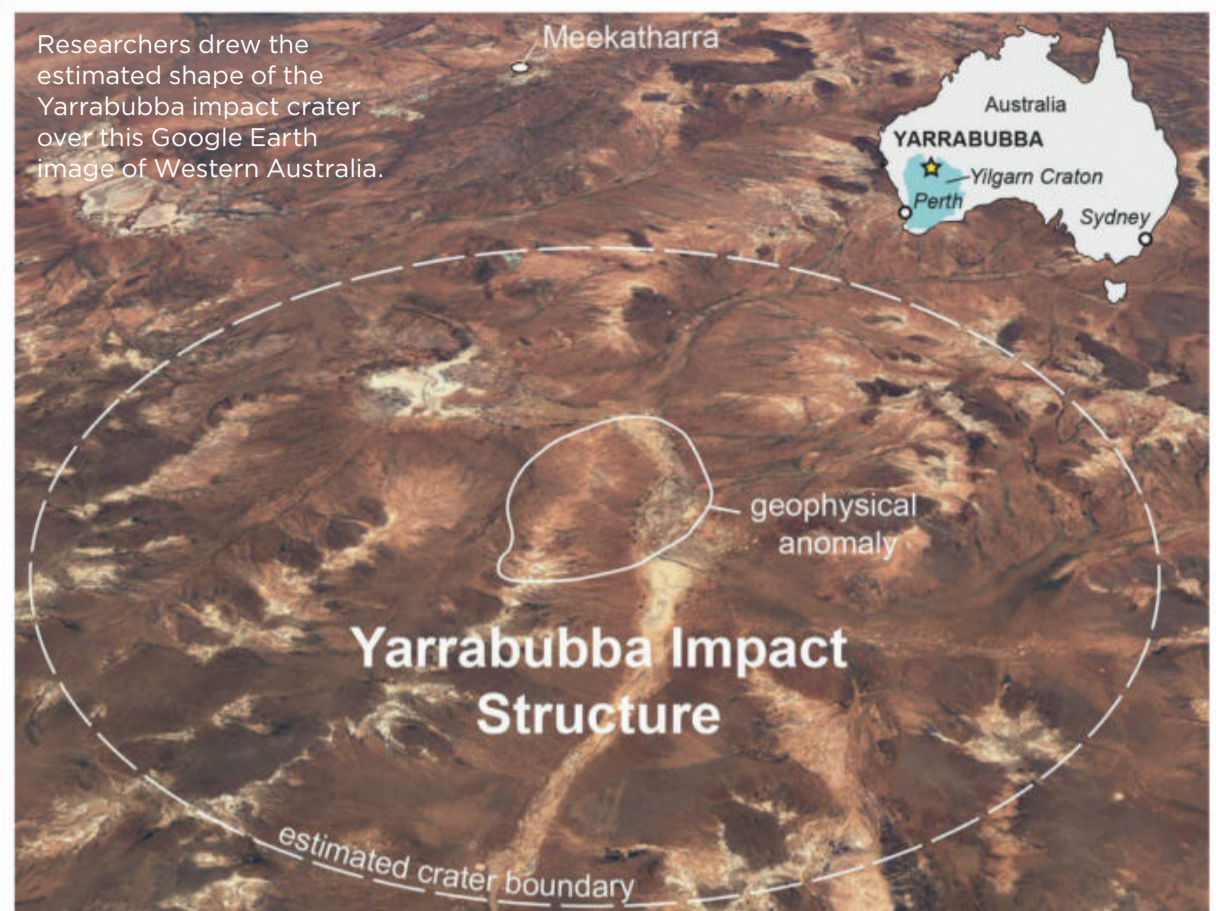
hold valuable information about the impact's age.

"[Barlangi Hill] has been interpreted as an impact-generated melt rock," the researchers wrote. That means its rocky innards hold mineral grains that were smashed, melted and eventually recrystallised by the ancient impact. Narrowing down the ages of those crystal inclusions, known as neoblasts, could reveal the date of the impact itself.

To do that, the study authors looked for neoblasts in a sample of grains containing two minerals, monazite and zircon, collected from Barlangi. Using a method called uranium-lead dating, which can reveal a mineral's age based on how many uranium atoms have decayed into lead, the team determined that the crater was formed roughly 2.229 billion years ago, making it 200 million years older than any other known crater on Earth.

## Exoplanet's atmosphere is melting before our eyes

KELT-9b, a hot Jupiter, orbits its sun so closely that a year there lasts just one-and-a-half Earth days. With a surface temperature of 4,300 degrees Celsius, KELT-9b is hotter than any other exoplanet, as well as some stars.

Astronomers discovered this supremely sweltering world orbiting a star some 670 light years from Earth in 2017, and are still learning details about just how unhabitable it is. For example, KELT-9b is so hot that its atmosphere seems to be constantly melting on one side, a new study suggests.

In a recent study published in the astrophysical journal *Letters*, researchers watched KELT-9b through NASA's Spitzer space telescope, which observes space in infrared light. This allowed the team to record subtle variations in the planet's heat as it whizzed around its home star.

Because the planet is tidally locked – meaning the 'dayside' always faces the sun while the other side always points away in perpetual night – the team saw remarkable differences in temperature on either side of the planet. Using computer models, the researchers determined that gas and heat were being cycled across the two halves of the globe, resulting in a dramatic circle of atomic destruction and rebirth.

On the dayside, the heat of the sun was so intense that hydrogen molecules in KELT-9b's atmosphere were literally being ripped to shreds and blown across the planet, a process known as



© NASA/JPL-Caltech

dissociation. While the nightside was still extremely hot at 2,300 degrees Celsius, it appeared to be just cool enough for loose atoms from the dayside to recombine into hydrogen molecules. Eventually, though, those molecules flowed back to the dayside, where they were ripped apart again.

$3,195, www.sony.com.au

# Sony A8G OLED

A beautiful – but expensive – OLED with best-in-class upscaling.

When it comes to OLED TVs, you probably think of LG – basically the only company in the world that produces enough panels at scale to supply the entire industry. But the TV manufacturers buying those panels (namely Sony and Panasonic) are taking the technology and making it their own with custom processors, in-house designed bezels and stands, as well as installing their own smart TV platforms – or in Sony's case, a licensed partner's.

The result is a TV that's different in both form, function and price from the TVs that LG produces, and are therefore worth looking at in more detail.

That leads us to the Sony A8G OLED that takes an LG OLED panel and infuses it with Sony's X1 Extreme Processor and Android TV Oreo with Google Assistant built into the TV itself.

Sure, it's slightly more expensive than the lower-cost LG B9 OLED and LG C9 OLED, but if you want the best upscaling, motion processing and picture



There's a physical power button and volume rocker located next to the ports on the back.

customisation options, look no further than the Sony A8G OLED.

## Design
Although it shares the same birthplace as the panels found in LG's B9 and C9 OLED TVs, Sony chose to encase that panel in a minimalist frame with a crescent-shaped stand. That gives it a slightly different look than the LG B9 OLED that uses a pedestal to hold the TV upright.

The stand is reversible if you want a slightly different look and,

in terms of cable management, you can string cords through the back of the legs of the TV, which should help to keep your entertainment center looking tidy.

While the bezel on the front is fairly minimal, the TV is a tad chunky in the back-midsection. That's where the internals of the TV are hosted, and that's where you'll find the IO ports, which are rather generous in quantity: On both the 55-inch and 65-inch versions of this TV you'll find four HDMI ports with HDCP 2.3 and one with ARC, plus a digital audio out, 3.5mm auxiliary and three USB ports.

For the real TV enthusiasts out there, the Sony A8G doesn't support eARC, nor does it have any HDMI 2.1 ports – but that's something that could be changed on the upcoming Sony A8H that's due out later this year.

## Smart TV
### (Android 8.0 Oreo)
Like the A9G OLED, the step-down A8G uses Android Oreo – the latest version of Android TV that supports built-in Google Assistant and a familiar row-based design that helps separate Android TV from smart TV platforms like Tizen and webOS.

Other TVs might have ruined Android TV for you – as some TV's processors just aren't capable of keeping up with the platform's resource-intensive visuals – but on the A8G  everything is snappy and responsive, with a relatively deep catalog of apps that can be found along the bottom-most row.

Each row is a visual representation of content inside an app. For example, the YouTube row will have recommended YouTube videos for you based on what you've watched previously. The same is true for the Netflix, Google Play Movies & TV and Play Music rows, too.

This design makes finding new content relatively easy, but it can bury the library of apps which now requires a bit of scrolling to get to. Among the supported apps you'll find Disney Plus, YouTube TV, Amazon Prime Video, Vudu, Crunchyroll, CBS All-Access, ESPN, Starz, HBO Now and many, many more.

## HD/SDR Performance
Any old 4K TV can take Ultra-HD content and make it look great, but the Sony A8G is among a select few that can take any content, regardless of age and quality, and make it shine. That's due primarily to the X1 Extreme Processor which uses a multi-faceted upscaling process to reduce grain, sharpen edges and enhance colors. This is something all 4K TVs do to some extent, but almost none of them do it as well as Sony does.

To test the A8G's mettle, we threw on *The Lord of the Rings: The Fellowship of the Ring* on DVD – a classic that's well-worth re-watching every few years. The result? The Shire, which has always looked picturesque thanks to its New Zealand backdrop, looked especially verdant on the A8G, with beautiful greens and bright blue skies, and the forest of Lothlorien and the Mines of Moria had an almost ethereal look to them – which we loved.

## 4K/HDR Performance
While OLED TVs have been panned in the past for their lower-than-LCD levels of brightness, the A8G will surprise you with 800 nits of peak brightness. That's still less than, say, a Samsung Q90 QLED or Vizio P-Series Quantum X, both of which easily top 2,000 nits – but it's a big improvement on previous generations.

That perceived uptick in brightness means that the A8G looks great in both dark settings and light-splashed living rooms, and helps HDR content look more colorful and impactful.

That said, Sony is fairly conservative when it comes to its color grading and tends to be less vibrant than other manufacturers. Image presets comprise Vivid, Standard, Cinema, Game, Custom, Graphics and Photo, with Standard being fairly versatile and applicable in most circumstances.

The A8G's stand can be reversed if you want to give your TV a different look.

★★★★⯪

The Sony A8G OLED is a fantastic 4K HDR TV with amazing picture performance, incredible upscaling and the best-in-class motion processing. We have some reservations about Sony's Acoustic Audio Surface tech and the plastic remote that uses an IR blaster to control the TV, but it performs in the only category that matters: picture quality.

Nick Pino
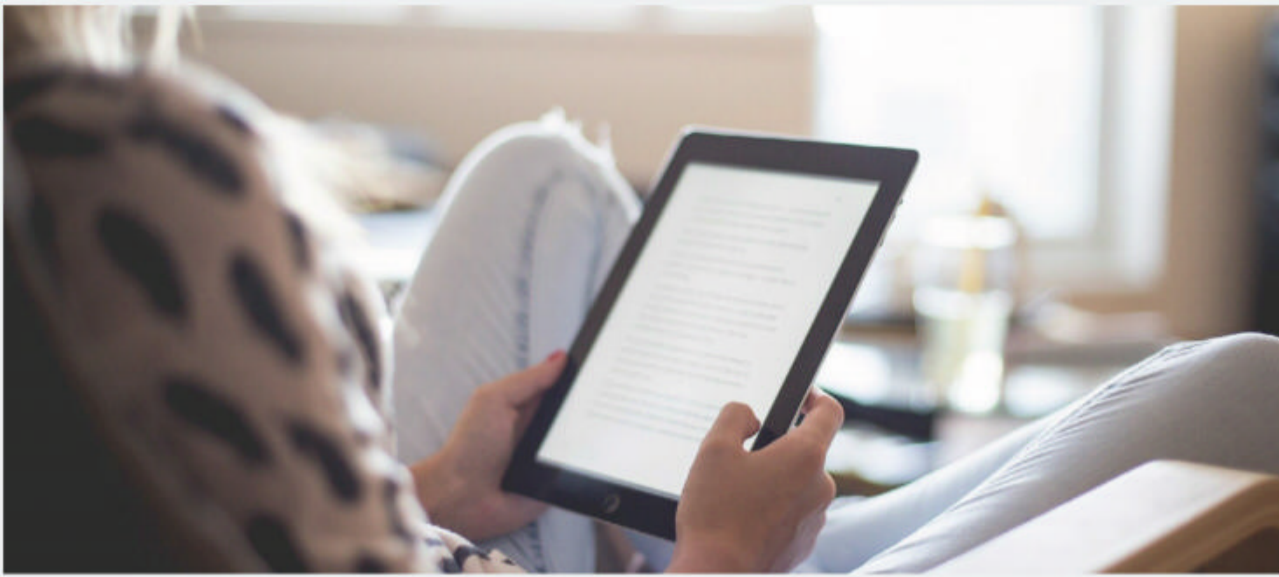
# Everyone's talking about: Big time online tracking

How much data are companies storing about you – and what exactly are they doing with it?

When you use any device, from your laptop to your phone, you leave traces. These can be physical — greasy fingerprints on a screen might lead a clever attacker to decipher your PIN code — but they're most likely invisible. Many large companies (including the likes of Google, Microsoft and Amazon) incorporate tiny trackers into just about every website you visit, offering helpful services to website owners in exchange for a little information on what you've been up to. If you've ever wondered just how Amazon can show you a month's worth of toaster adverts after you once looked up the temperature of bread, that's why.

Many trackers are not just online; unless you opt otherwise, Microsoft will keep information on the way you use Windows 10, Google will remember your search history, and Amazon is looking at far more than just your shopping preferences. If you use a Kindle, for example, it turns out Amazon will keep a record of literally every tap you make on the screen. The company says this is in an effort both to improve its software — it noticed that people were flicking back and forth between pages to reference previous material, and has introduced a new feature to make this easier — and to keep its Whispersync virtual bookmark service in line. It'll also store your Alexa activity which, if you're a user of an Echo device, you can check out at **amazon.com/alexaprivacysettings**.

Crucially, we've agreed to much of this tracking, whether deliberately or not. When a website flashes up that annoying 'we use cookies' button, that's not by choice. Legally those sites are forced to tell you they're tracking you, and you should be able to dive in and find an option through which you can disagree to any terms you're not happy with. When you're setting up a new device, or a new copy of Windows, you also get the option to switch off those things which make you uncomfortable. While these companies keep doing it — and they will — we'll keep talking about it; tracking isn't as sinister as it sounds, but it is, for the most part, optional. **TL**

## The 60–Second Quiz
**Pens at the ready, your time starts now!**

**01** Visiting video.com will lead you to which company's website?
**A** Disney
**B** YouTube
**C** BBC

**02** Where does visiting windows.org lead you?
**A** Microsoft
**B** Autoglass
**C** Saint James Chapel, Chicago

**03** Let's try another – where does go.com lead?
**A** Go Compare
**B** Go Outdoors
**C** Disney again

**04** Sticking with a theme, where do you end up if you visit wallet.com?
**A** PayPal
**B** Google Pay
**C** Apple Pay

**05** Which company owns the web address microsoft.sucks?
**A** Microsoft
**B** Apple
**C** Google

**06** Lastly, which of these takes you to the Amazon website?
**A** awake.us
**B** awake.com
**C** awake.org

## Everything www.voidtools.com

There are times when you're desperate to find a specific file and Windows' own search function is more interested in showing you a web link to something irrelevant. Voidtools' Everything is a neat alternative – it starts (after a little grunting and groaning to update its index) by showing you every single file on your PC, then narrows down its results as you type.

You'll need to know a little about the filename you want to find if you expect to find it quickly, but you can use the search term 'content:' to dig through the content of documents if you need a little more granular searching and don't mind waiting a while for the results. Really, that's not the point: Everything is a tiny program that makes absolutely minimal impact on your system, and it does a much better job of searching than the built-in tool.



Everything really does mean everything – prepare to be overwhelmed.

# The news in numbers

Here we reveal some mostly useless yet highly fascinating numerical facts...

## 27,000

The number of folds it took to break the hinge in Motorola's new foldable Razr phone, in testing by *CNET*.

## 22GWH

Is the amount of renewable energy A G Barr has sourced from wind generation to power its energy drink factories.

## 2030

The year by which Microsoft expects to have become carbon negative – aiming to remove from the environment all the carbon it has emitted since 1975.

## 2050

The year by which the UK's NHS hopes to be carbon neutral, according to plans

## 2035

The year by which new petrol, diesel and hybrid cars will be banned from being sold in the UK, according to government plans.

## $1 billion

The revenue earned by Twitter in Q4 2019, the first time it's hit that figure.

$3,499, www.panasonic.com

# Panasonic Toughbook 55

A surprisingly practical and modular platform.

There are lots of working environments were normal computer equipment wouldn't survive for long. Those in the military, or working with a disaster support agency, or even on a construction site can't have a mission-critical computer die because of rain, or dust.

For those applications, something beyond a typical Ultrabook is needed. Having had the Panasonic Toughbook 55 for a couple of months, we'll state from the outset that this machine is a highly tuned answer to the problems we've mentioned, and dozens of other situations.

There's a price to pay though. Our review machine was over $3,000. Cheaper variants with HD non-touch screens are available.

### Design
It's a cliché, but all toughened computers need to have visible screws, and the Toughbook 55 has plenty of those. However, what most purchasers will notice first is that this isn't a slim and elegant design. It's a chunky and angular piece of technology that is dominated by a substantial carry handle at the front.

Behind the handle is a central touchpad with two thumb-activated buttons that extends to the very edge of the keyboard area.

Panasonic provided a well-proportioned keyboard where the keys aren't flush against each other, and there is still room to the left and right for narrow borders

> *It's a cliché, but all toughened computers need to have visible screws, and the Toughbook 55 has plenty of those.*

under which the speakers live.

While thicker than normal, this doesn't appear a radical departure for laptop layout, until you realise that it has no visible ports. None.

There are ports, more than we imagined, but they're all safe behind protective doors and covers that enable this design to achieve IP53 dust and water resistance and meet the US military's MIL-STD 810H requirement. We wouldn't leave one exposed to rain for an extended period or buried in sand. But these protections should keep it from failing at the drop of rain or being dropped.

But the true revelation is a level of user-installable upgrades and options that would make a

standard Ultrabook hang its head in shame.

In the standard box, along with the laptop, you get a single 6500mAh battery. The battery fits into one of two slots on the front left and right, and you can use either one. That not only allows for dual batteries, but Panasonic has modules to add fingerprint reading, a Smart Card slot or an RFID reader into the same receptor.

And this isn't the only optional slot; there are two others, the Selectable I/O bay and the Selectable Universal Bay. On our machine these weren't populated, but the I/O bay can be used to add VGA, extra USB and a second Gigabit LAN port, while the Universal bay can take an optical drive, another Smart Card reader and even a discrete GPU. In terms of customising the Toughbook to meet the needs of a project, this approach allows for more flexibility than we've come to expect from a laptop. Of course, all these need paying for, adding yet more to the already high cost.

Panels on the underside allow easy access to the RAM slots and the single M2 storage module, enabling those to be easily swapped for larger capacity parts. For those IT staff concerned whether so much access to the internals would be a good thing, Panasonic engineers cleverly included holes for security bolts to be installed to stop the curious from unfettered exploring.

Our review model came with a touchscreen, and hidden in a spring–loaded silo is a stylus for those that don't like oily fingerprints on their display.

## In use

Normally a laptop that weighs 2.1kg wouldn't be easy to carry, but the integrated handle makes transporting this one easy. That's helpful, because if you add the second battery the complete package is 2.47kg, and that doesn't include the power supply or any other accessories.

For those wanting a long time away from power, Panasonic makes a battery charger that can take four batteries. The cells are hot–swappable, and with two bays free, the machine doesn't need to be shut down while a fresh one is switched in.

In retrospect, it might have been smarter to build the fingerprint reader into the machine and leave the bay it occupies for other things, but how much you agree with that is probably dependent on how important the security aspects of this design are to you. For those who need a highly secure system, there are plenty of options available here.

## Performance

The 8th generation Intel Core i5-8365 vPro processor is a stalwart for laptop makers, delivering good performance without undermining the battery life with superfluous cores or crazy boost clocks.

The numbers revealed by benchmarking show that it doesn't do anything extraordinary in this machine, but it delivers solid scores that match other solutions built around the same platform. The only numbers that disappointed in our tests were those associated with the storage. The review machine was fitted with a SATA

Nothing looks quite as unique as Panasonic's Toughbook.

M2 SSD, not an NVMe model, reducing the read and write speeds to 540 MBps and 500 MBps respectively.

Where this machine truly shines is its battery life. Panasonic quotes 20 hours of life from a single battery, a wildly optimistic figure, but even in our PCMark 08 Home test we managed more than 10 hours. That's continuous use, so unless you can work that long without a break, it should last even longer in the real world. And, when you can potentially add another battery, and carry more, that could extend usable running time into days or even a week.

For those that can't easily access mains power for prolonged periods, this could revolutionise their computing use.

It does many things well, but the two standout aspects are the modularity of the design, and what that enables from a security perspective. It enables customers to customise the hardware in a way that doesn't involve the maker having an inordinate number of different SKUs and allows the machine to be smartly repurposed during its working life.

The combination of protection and flexibility is a winner.

★★★★☆

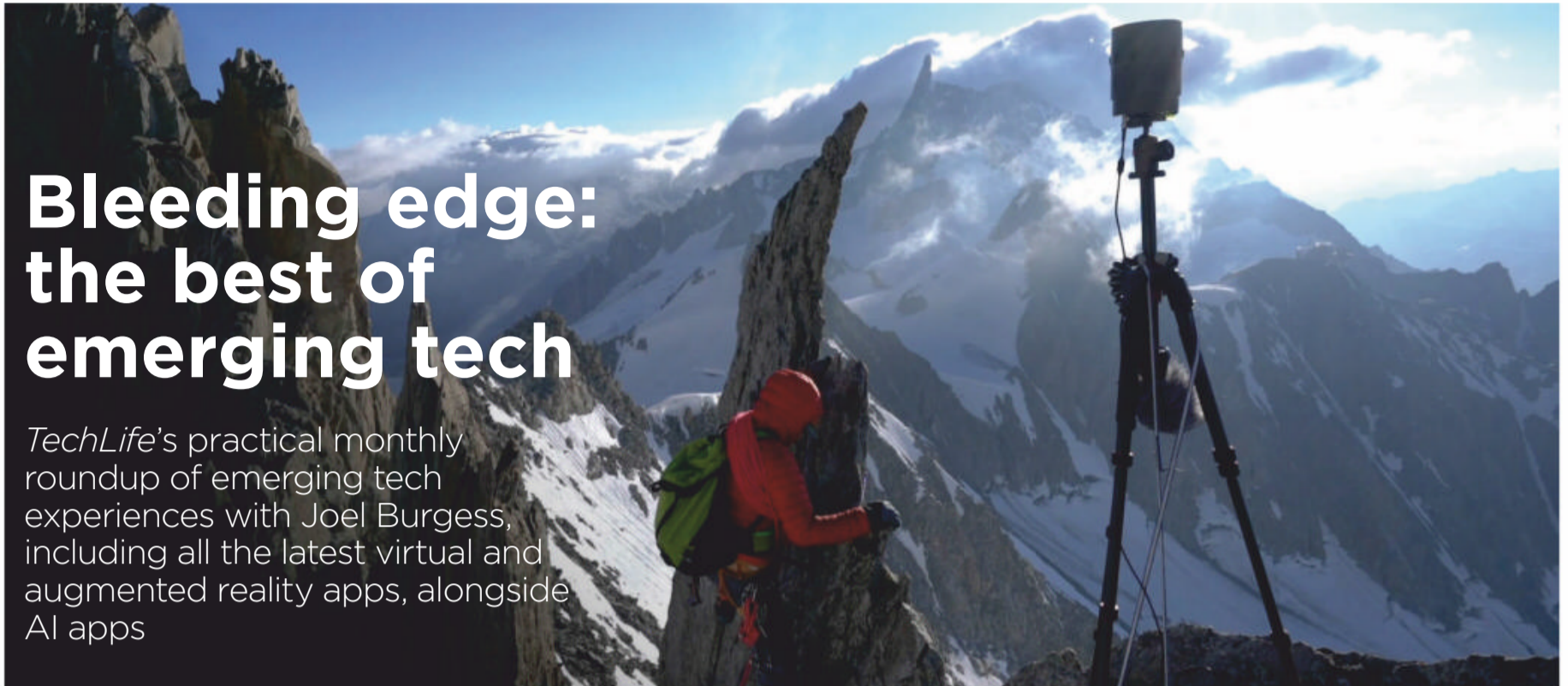An amazing piece of engineering, the Toughbook 55 is a go-anywhere computing platform. TechLife

**CPU** Intel Core i5-8365U vPro
**GPU** Intel UHD Graphics 620
**RAM** 8GB
**Storage** 256GB
**SSD** (SATA only)
**Screen** 14in 1080p
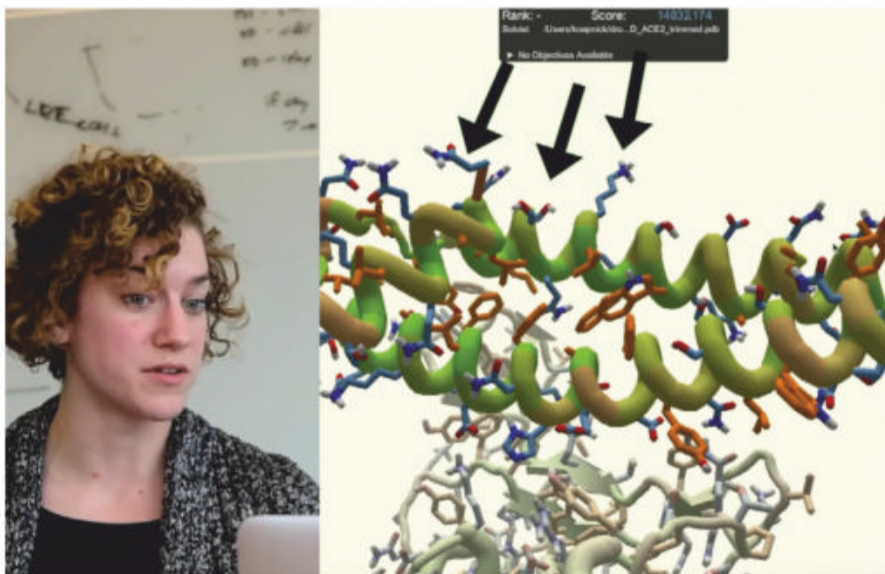**Connectivity** Wi-Fi 5, Ethernet, Bluetooth 5.0, 4G LTE

# Bleeding edge: the best of emerging tech

*TechLife*'s practical monthly roundup of emerging tech experiences with Joel Burgess, including all the latest virtual and augmented reality apps, alongside AI apps

The coronavirus is having a large impact on the technology industry, and the emerging tech scene is not immune to it. But the industry is fighting back with autonomous robots that are helping Chinese hospitals curb the spread of COVID-19 by performing menial tasks, AR games designed to help find a vaccine, and a fully online VR conference platform that hopes to fill the gap of cancelled tech events like MWC. Apart from all the pandemic related emerging tech this month there's also some updates on how the Australian Federal Police and non law enforcement investors have had access to Clearview AI's facial recognition technology… just in case you still had any hope left for the future.

## VR
### Everest VR
$15, oculus.com

If you've ever wondered what the view from the top of the world is like, *Everest VR* is sure to pique your interest. The immersive video project follows John Griffith and Sherpa Tenji in their journey to finish a climb of Everest and Mt. Lhotse without any bottled oxygen. The challenging feat was originally conceived by a friend and fellow climber Ueli Steck, who died while preparing for the journey. The full length 8K stereoscopic 3D feature can be purchased for VR headsets through the Oculus store and includes five iconic settings for major experiential scenes along the way.





## AR
### Foldit
Free, fold.it

In 2011 a game created by the University of Washington's Center for Game Science led to some major breakthroughs in viral research that had eluded medical researchers for decades. The team behind this 3D protein key building game, *Foldit*, have created a new edition that hopes to get creative gamers to come up with molecular solutions to slow or halt the transmission of the novel coronavirus COVID-19. Anyone is free to download and play this challenging puzzler and because it is just shape-dependent, you don't even need to have any medical knowledge.

## AI
### Wildlife Alert
$TBC, https://apps.wcswildlifetrade.org/

While we might be familiar with things like the ivory trade, everything from exotic parrots to reptiles are traded and trafficked on the black market, depending on global supply and demand. So instead of using 'the stick' to police this market, conservation criminologist Dr. Meredith Gore wants to use AI. The Department of Fisheries and Wildlife professor at Michigan State University hopes to use situational crime prevention techniques and AI processing to reduce the appeal of animal poaching before anything is killed.

**VR**

## Run the World

25% of ticket sales, runtheworld.today

With every tech conference from MWC to Google's I/O conference falling to the threat of the novel coronavirus, there's perhaps never been a better opportunity for the virtual conferencing company Run the World to showcase the merits of digital conference. The platform has been described as "a hybrid of Zoom video, Eventbrite ticketing, Twitch interactivity and LinkedIn networking" by an early investor… a combination that sounds like a pretty good alternative to a real–world conference. Run the World recently held the Hack for Wuhan digital hackathon conference that attracted 875 contestants and held virtual conferences for more than 500 audience members.
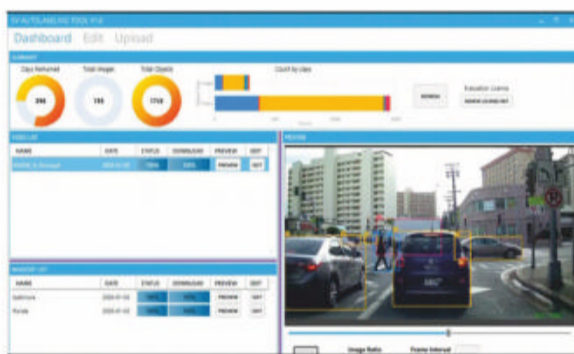


**AI**

## StradVision

$NA, stradvision.com

In the US there are over 1.5 million deer–related vehicle collisions every year causing, on average, 200 fatalities, 10,000 injuries and over US$1bn in damages – which is a pretty big incentive for good animal avoidance systems in autonomous vehicles. In response to this, camera perception company StradVision has updated its advanced driver assistance AI systems to better recognise animals. The company's CEO has said the software will "almost completely end" animal related road incidents.



**AI**

## Promobot Terminator

US$25,000, robo-c.ai

Former Governor of California and actor Arnold Schwartzenegger is suing a Russian robot manufacturer, Promobot, for creating a humanoid robot bust of his face that consumers can buy for US$25,000. Complete with twitchy, unnatural facial expressions the Arnold Schwartzenegger robot will greet guests, turn the kettle on and make you feel like your smarthouse is one rogue download away from murdering you while you sleep.

## Robots help prevent coronavirus spread

Hospitals in China are using three robots to help deliver food, sanitise public spaces, and provide directions to visitors in order to limit the spread of coronavirus in highly affected areas. While there is limited evidence right now, they all reduce instances of contact between humans both with the virus and without. One US company called Draganfly is beginning to use its drone to make remote diagnoses of patients suspected to have contracted the virus.

## Clearview used by non–law enforcement investors and the AFP

The CEO of the controversial AI facial recognition company Clearview said on Fox Business that the app was "strictly for law enforcement", however a *New York Times* investigation found that the company has actually made the software available to major civilian investors over the last year. Grocery store magnate John Catsimatidis was quoted as having unfettered access to the software in 2018, and actor turned investor Ashton Kutcher bragged on the talk show *Hot Ones* about having a facial recognition app on his phone with the exact same feature set. According to a *Buzzfeed* report the Australian Federal Police were also on a leaked client list for the company.

## Microsoft and IBM sign the Pope's AI pledge

While you might not consider the Vatican as the most informed authority on tomorrow's technology, when the head of the Cathloic church suggests that tech companies should impose ethical restrictions on the development of AI many, it seems, still listen. Both Microsoft and IBM signed Pope Francis's 'Rome Call For AI Ethics' pledge that asks tech companies to ensure that AI technologies like facial recognition don't erode the rights of the underprivileged. **TL**

# Best new apps

James O'Connor reviews the most interesting new apps for iOS and Android.

## Microsoft Office

Free to download
iOS, Android
office.com

The newly consolidated Microsoft Office app now collects everything into one place, so you can organise your Word, Excel, and PowerPoint files all in one place, as long as they're uploaded to the cloud. This means that you no longer need to have three separate apps on your phone or tablet, which makes things a bit tidier. You can work on your files or make new ones from the app, too, and it works much better than the atrocious Google Docs app (although unfortunately you can't share files so easily as you can through there). Is the Microsoft Office app a perfect substitute for using these applications on a home computer or laptop? Not at all – trying to build a PowerPoint on a phone is a nightmare. Is it a great way to keep track of your files and make minor changes on the go? Absolutely, and having all your files in one app is handy. Microsoft Office might not be the most exciting app on your phone, but it'll make working away from your desktop a lot easier. ★★★★☆

## Dr. Seuss' ABC – AR Version!
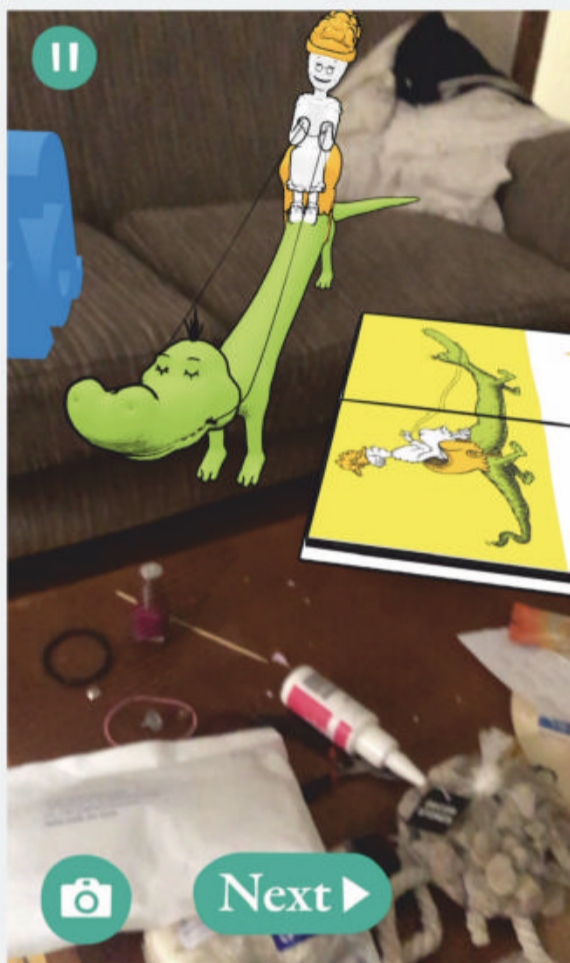
$5.99
iOS, Android
www.seussville.com/

*Dr. Seuss* comes alive in this AR app, but there's no rambunctious cat monsters or haughty tree spirits for your children to deal with here. This is aiming at the good doctor's very youngest fans – it's a simple app designed to help them learn how to spell out the alphabet. Your child (or you, if you're an adult who reviews apps for a magazine) has to trace out each letter with a finger, in both capital and lower-case forms, before being rewarded with a small AR scene of Seussian creations cavorting. This is a Seuss product, of course, so expect plenty of alliteration – spell out B and you'll get "barber baby bubbles and a bumblebee." It's neat, but don't expect your kid to be super engaged, or to, necessarily, like it more than a regular book (it's certainly more complicated to read, and it's not really teaching them how to write with a pencil). There's a playground mode too, where you can stamp AR critters all over the room, which is neat fun. ★★
★☆☆

## RTRO – Camera by Moment
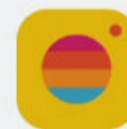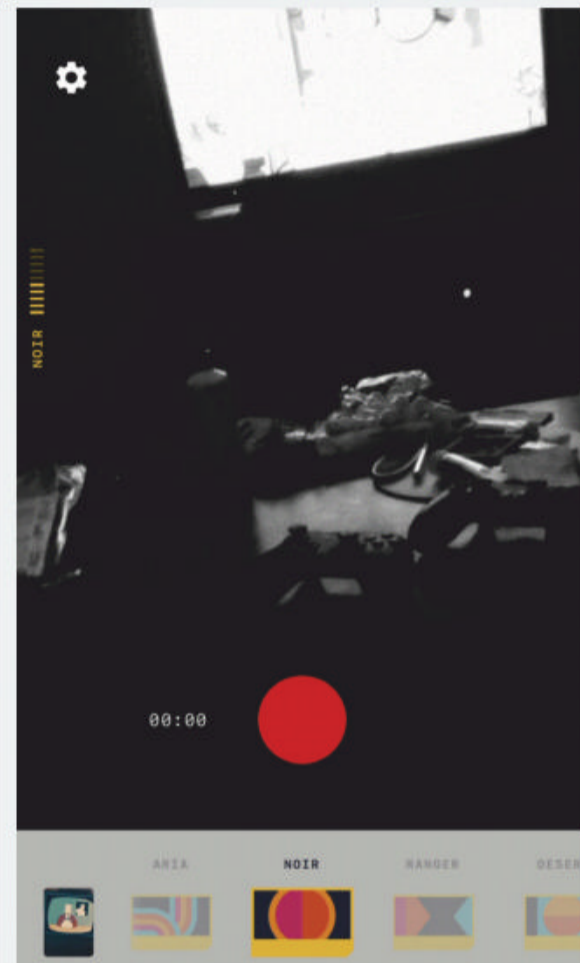
Free
iOS
www.rtrocamera.com

RTRO is a video filtering app that lets you apply numerous different looks to your footage (a few of which are free, although others are paywalled), pick between aspect ratios, and then record up to 60 seconds. This is all well and good, but there are some confusing decisions here. "Shorter is better," the app's site explains, which is why you're limited to 60 second shoots – but I'm not convinced that 60 seconds is short enough to constitute a gimmick or long enough to serve as a useful length in all circumstances. Switching between video and photo modes is needlessly cumbersome, too. The limited selection of retro filters and ratios is neat, and I liked the look of the videos I took, but I also can't imagine RTRO becoming a mainstay in my photo/video app folder. It's a bit of fun to play around with, but – as with many nostalgia apps – I am not sure that it has real long-term legs for extended use. ★★★☆☆

## byte

Free
iOS, Android
byte.co

Byte is, apparently, the new Vine. I thought that Tik Tok was the new Vine? As far as I can tell, two things are true here – I am very old, and these are all the same damn app, with the main difference being that byte's looped videos run just 6.5 seconds to Tik Tok's 15. This means that the videos on Tik Tok are given a bit more breathing room, and, in theory, folks making things on byte need to be economic, getting to the point of their video as fast as possible. There's a very specific cadence to the videos that byte's users are making; they've been trained by society in the art of being short and sharp, and bless 'em, scrolling through byte is fairly delightful as a result. The app separates videos into broad categories, and it's a great way to pass 5-10 lazy minutes on an otherwise quiet afternoon. Will we start to see a new wave of byte comedians emerge like we did with Vine? Time will tell, but for now it's a lot of fun. ★★★★☆

## Finder

Free
iOS, Android
finder.com.au

Finder is the app equivalent of eating all your vegetables – it can feel like work, especially when dessert is in the freezer (or the games folder), but the further into adulthood you are, the more aware you are of its importance. Hand your bank information over to Finder and it'll itemise your bills based on the information it gleans from your accounts, chart your expenses, tell you whether the total sum in your bank has gone up or down that month, and generally help you be fiscally responsible. It's also, much like the website, a huge repository for deals, rates, and prices for all manner of essential services. I found that its ranking of prices was sometimes a bit off, and that it's not a replacement for proper vetted recommendations, because it focuses so much on prices. Don't believe the app when it tells you to sign up for TPG over Aussie Broadband, for instance. Because of this, Finder probably won't overhaul your life – but it will paint a pretty accurate picture of how you're living. ★★★☆☆
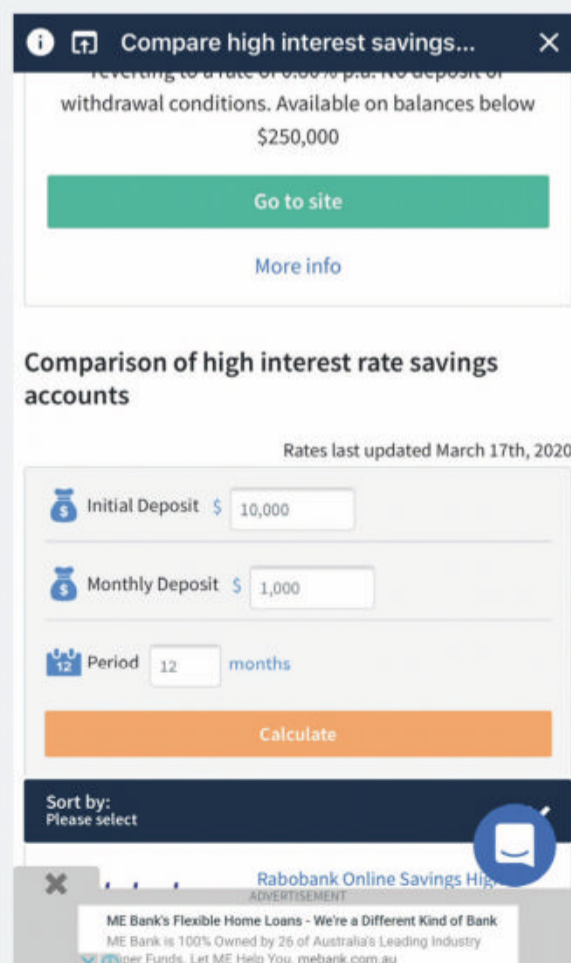
## DarkRoom – Photo Editor

Free
iOS
https://darkroom.co/

DarkRoom has been around for a long time, but it recently received a major update to its rendering engine that deserves fresh eyes. Indeed, it's a pretty potent, powerful photo editor, whether you're using the free version or splurging US$33 a year on the pro version (which is certainly worth it if you're editing a lot of photos on your phone or tablet). Editing your photos is incredibly easy and intuitive, and even as a (very) amateur photo editor I found that I could make my photos more dynamic or moodier with just a few tweaks. The free version is very generous with how much it will let you do, too. It's easy to undo changes, and to save your pictures, export them, or slap a watermark onto them. Darkroom is a fairly serious-minded app, so don't expect sticker packs or serious photo manipulation – it's all about getting your shots looking as good as possible. It's a lot of fun to mess around with, but more serious photographers will find these features handy on-the-go, too. ★★★★★
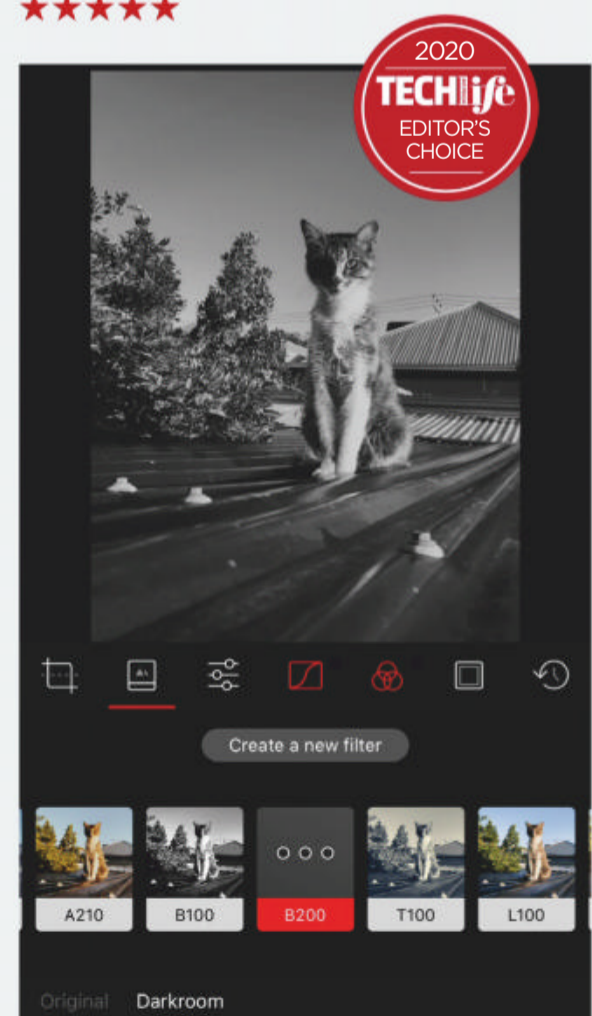
## *Gears 5* will be optimised for Xbox Series X

The Coalition's Mike Rayner showed off the opening cutscene of *Gears 5* running on the Xbox Series X with Ultra settings – the same used for the PC version of the game. The version Rayner showed off has a 50% higher particle count than the PC specs and higher texture resolutions. It also runs at 60 fps in 4K, which is double the frame rate of the Xbox One X, and the team is looking into a version that would run 120fps for multiplayer games.



## *Control* DLC *The Foundation* gets June release date on Xbox One

*Control*'s first big paid expansion, *The Foundation*, is coming to PS4 and PC on March 26, and on Xbox One on June 25. We've known the new *Control* DLC would release on March 26 as a PS4 timed-exclusive, but it's news that it's coming to PC, via the Epic Games Store, on the same day. We also know now that Xbox One players will need to wait a whole three months longer for *The Foundation* than PS4 and PC players.

# *No Man's Sky* developer to release new game *The Last Campfire* this summer

New indie adventure coming down the trail.

*The Last Campfire*, Hello Games' first project since releasing *No Man's Sky*, is launching this summer for Nintendo Switch, PS4, Xbox One, and PC.

A new trailer was revealed during the latest *Nintendo Indie World Direct*, which revealed the platform information and release date.

First announced at The Game Awards in 2018, the adventure follows Ember, who is on a journey to light the titular last campfire. Expect some puzzles and tears as Ember embarks on their quest, which you can get a glimpse of in the trailer below (maybe make sure you're emotionally ready for it first).

This smaller scale project is clearly a departure from Hello Games' sci-fi explorer, but we're really digging its somber but cute aesthetic. Lead character Ember almost reminds us of a Chibi version of *Journey*'s main character, while the game's light puzzling looks like it'll be pretty soothing. A line on the game's official website gives us a hint at where the story will be going, as it says, "Travel deeper into the lands beyond the dark forest and overcome the adversities before you."
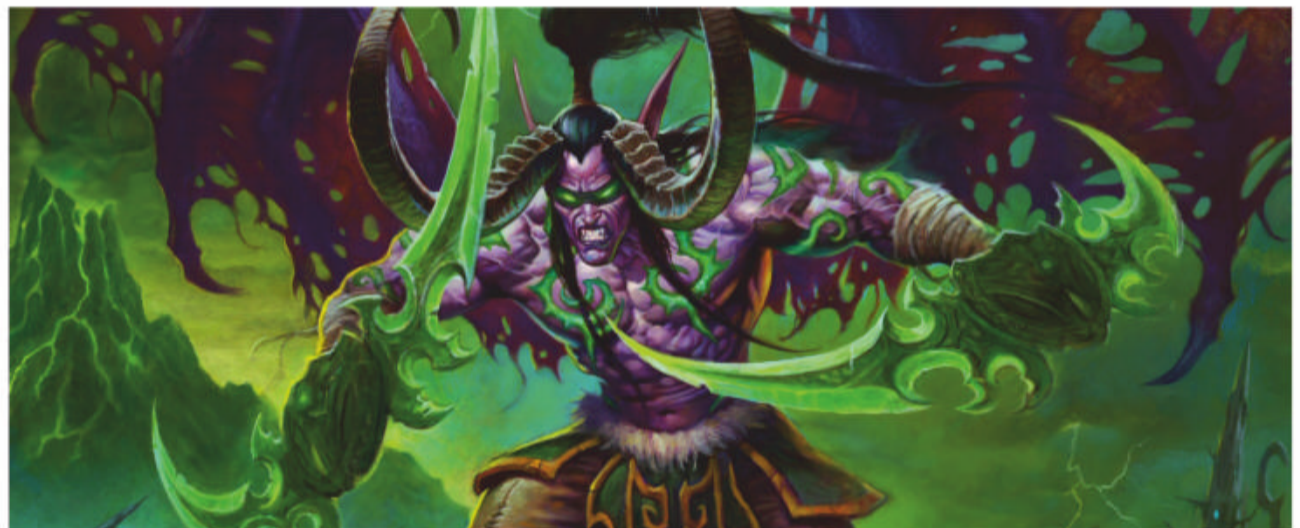


# *Hearthstone* Demon Hunter class coming this April will be free to all players

*Hearthstone*'s long-awaited 10th class is nearly here.

The *Hearthstone* Demon Hunter, a full-fat 10th playable class, will launch on April 7 alongside the Year of the Phoenix, Blizzard announced today. This is the first new class in the six-year history of *Hearthstone*.

Players will get to know the Demon Hunter, played by Illidan Stormrage, starting on April 2 through a four-part single-player campaign. This will introduce Demon Hunter's class abilities while explaining the history of Illidan, AKA the brother of Druid hero Malfurion Stormrage. The campaign will conclude when the class officially launches on April 7.

This introductory campaign, and the Demon Hunter class itself, will be free to all players. Not only that, players will receive all 10 Basic Demon Hunter cards, plus 20 cards from the broader card pool. Demon Hunter will gain 15 cards per expansion throughout the Year of the Phoenix – 45 total, which is 15 more than the other classes – so while its card pool will be relatively small at first, it will grow rapidly. That said, its power level in the Wild remains to be seen.

# Xbox Series X controller revealed: share button, cross-compatibility, and more

Xbox worked to create "a next-generation controller to deliver what fans wanted most".

The Xbox Series X controller has been officially revealed, with confirmation it will have a share button, as well as work with older Xbox models.

The details came through Xbox Wire, who interviewed Xbox senior designer, Ryan Whitaker.

When the Xbox Series X was first revealed, we did get a glimpse of a controller that looks almost exactly the same as the current Xbox One controller. Will Tuttle, editor-in-chief on *Xbox Wire*, explains that the fans love for the current controller resulted in the team wanting "to ensure they didn't change things for the sake of change," and to instead build on the Xbox One controller in "smart evolutionary ways" that would still allow players to retain the muscle memory they've built up over the years through using the current-gen controller.

"The Xbox design team developed a next-generation controller to deliver what fans wanted most: improved ergonomics for a wider range of people, better cross-device connectivity, easier sharing, and reduced latency," Tuttle states.

## Cross-compatibility
Cross-compatibility is a big factor

in Xbox's shift to next-gen, and Whitaker states that there will be support for cross-compatibility between Xbox Series X and Xbox One controllers and consoles:

"They all work together with the same great Xbox Wireless Radio. Gamers can also play on more devices including PC, Android, and iOS. We're implementing Bluetooth Low Energy (BTLE) so that pairing to these devices is much easier. The new controller also remembers multiple devices so switching between them is more seamless. And a USB-C port allows gamers to play and charge with a modern cable that's more readily available."

Compatibility and connectivity were key areas when it came to the design of the new controller. "The new controller needs to work equally well on Xbox One and pairing and moving between all these devices needs to be easy," Whitaker says. The controller is described as a "common touchpoint for your Xbox games across all devices" and it's specifically designed with interconnectivity in mind.

## Easier sharing
One of the controller's most noticeable changes is the inclusion of a new Share button. Whitaker

*"The angles are finely tuned to give you a good amount of leverage with minimal movement. Gamers will notice a performance boost right out of the box."*

shed some light on why Xbox decided to add the button to the Xbox Series X controller, saying "adding a Share button is the best way to make capturing and sharing instantaneous. It's easy just to grab a screenshot or record a video without needing on-screen menus. Then you can easily access and share content with your favourite social platforms or directly with friends."

## Size and textures
The feel of a controller when you're holding it can really be, pardon the phrase, a game-changer. Xbox has added new textures and finishes to the next-gen controllers with a "tactile dot pattern on the triggers and bumpers, which provides grip to improve feel and performance during gameplay." .

The size was taken into consideration too. One of the key areas Xbox explored was ensuring the controller fits a wider range of hand sizes. "By accommodating hands similar to those of an average 8-year-old, we found we could improve accessibility and comfort for hundreds of millions more people without negatively affecting the experience of those with larger hands," Whitaker explains. **TL**

$99 | PC, Switch, PS4, Xbox | www.bethesda.net

# Doom Eternal

Screams at you to move faster and to fight harder, and you can do nothing but obey.

Much like its predecessors, *Doom Eternal* is a hammer-horror pantomime in which you are made an active participant. It is an elaborate and self-indulgent production, its violence so over the top that you can't help but smile as it spills out over the stage and under your feet. It's an utterly ridiculous and strangely endearing showing, warping your suspension of disbelief so extensively that you'll wonder whether you've crossed over to another dimension – to a world where the first-person shooter followed the archaic directions first outlined by *Doom* in 1993 without question instead of turning toward the teachings of *Half-Life*.

The problem with this stage show is that the screaming has to stop sometime. The director is hoarse and is begging you to enjoy an intermission from the action. The bullet casings need to be collected, they tell you; the buckets of blood need to be refilled, the gore mopped up, and the guitars tuned back down to D. The cast of cannon fodder needs to take a breather as the next hellish stage is reset somewhere out of sight. You were moving too fast, and there's still a little story left to shout into your face.

I can count the number of first-person shooters that can function competently as platformers on one hand, and *Doom Eternal* is not among them.

*Doom Eternal* routinely breaks the pace of its action by forcing you to stiffly navigate towering spaces at regular intervals. You'll do this by swinging imprecisely between monkey bars, scaling bland craggy walls, bouncing off of unstable platforms, dashing between spacious maws of death, and double-jumping to ledges with slippery collision detection. *Doom*'s movement systems are tightly refined, designed to keep your crosshairs focused on fast-moving enemies amongst a backdrop of colourful chaos.

If you like games that practically yell at you until you succeed... *Doom Eternal* is for you.

It's levels like Doom Hunter Base, Super Gore Nest, and Mars Core that make up the bulk of the mid-game that are hit hardest by this design decision. These spaces are larger and more ambitious than anything the studio has committed to before with *Doom*, and they struggle to maintain momentum.

First-person platforming just about works for *Doom* when it is an optional extravagance – when you're off exploring for the myriad of optional collectable scattered throughout each of the missions – but as a prerequisite to progression they only serve to introduce points of friction in an otherwise frictionless experience.

★★★⯨☆

Tries too hard to be too many things, but when it works there's no shooter like it.
Josh West

$79.95 | Switch | www.nintendo.com.au

# Animal Crossing: New Horizons

The ultimate getaway from reality.

As I grin at the simple pleasure of seeing Goldie, an old *Animal Crossing* favourite, pottering around her tiny one-room house in a Wee Willie Winkie–style nightcap and pyjamas, I realise how good it feels to be home. Not home in the sense of being curled up on the sofa in real-life, but that sense of comfort that comes from immersing myself again so deeply in the animalese world *Animal Crossing*. There's nothing that quite compares to the quiet, peacefulness of existing within the bright, simplistic world Nintendo's life simulator, and with *Animal Crossing: New Horizons*, that sense of the series being the ultimate getaway from reality is amplified tenfold.

That's not just because *Animal Crossing: New Horizons* has possibly arrived at the most perfect time – a period where many of us may find ourselves being trapped at home a little more than usual – jetting us off to an island paradise courtesy of Tom Nook. Yes, the money-focused tanuki is back with a new investment scheme, and this time it's about setting up a new life on a deserted island. Nook's in charge now

though, meaning you've been demoted to Resident Representative, and later when she eventually arrives like a sunbeam of cuteness, you realise Isabelle reports to Tom Nook now too. But that doesn't mean your powers to shape the future of your new sandy home is any lessened. There are actually a slew of new features to help you execute your own vision of paradise,and the moment Tom Nook steps back and relinquishes island control to you, you're ready to create your ultimate desert getaway.

In a world where you can spend hours on end looping short, pacey in-game days in *Stardew Valley*'s farming simulation, *Animal Crossing* is still tied to the real world passing of time. Initially, this means the pace of *Animal Crossing: New Horizons* feels incredibly slow, but, this is a game designed to be played as much, or as little, as you'd like on any given day.

★★★★⯪

A game that takes its time, but is thoroughly worth waiting for.
Sam Loveridge

---



US$31.95
PC, PS4, Xbox
www.rugby-thegame.com

## Rugby 20

THE WAIT FOR A TOP-NOTCH RUGBY GAME GOES ON – BUT THIS IS OKAY, DESPITE ITS FLAWS.

No sport is tougher to translate into a videogame than rugby union, and the welcome news is that *Rugby 20* is able to string a few passes together even if it ultimately gets stuck in a ruck. Two teams of 15 players on the field, all of whom have bespoke roles, slinging around a funny-shaped ball, with the nuances of rucks, mauls and line-outs to consider: little wonder even EA's megabucks haven't gone anywhere near the sport for 13 years. As such, you have to credit developer Eko Software for even chancing its arm at such a complex pastime. Sadly, games aren't purchased on effort alone.

Those who open their wallets in exchange for *Rugby 20* receive a true oddity in return. Because, well, it's a little bit crap – yet also kind of unputdownable. A bit like sour sweets: with every bite you wince, and yet still you find yourself reaching for another, time after time. It's certainly better than the utterly woeful *Rugby 2018* that we previously awarded 1 out of 5 stars. In *Rugby 2020*, however, a stubborn battle with the game's mechanics is one of the things that keeps you coming back for more.

★★⯪☆☆

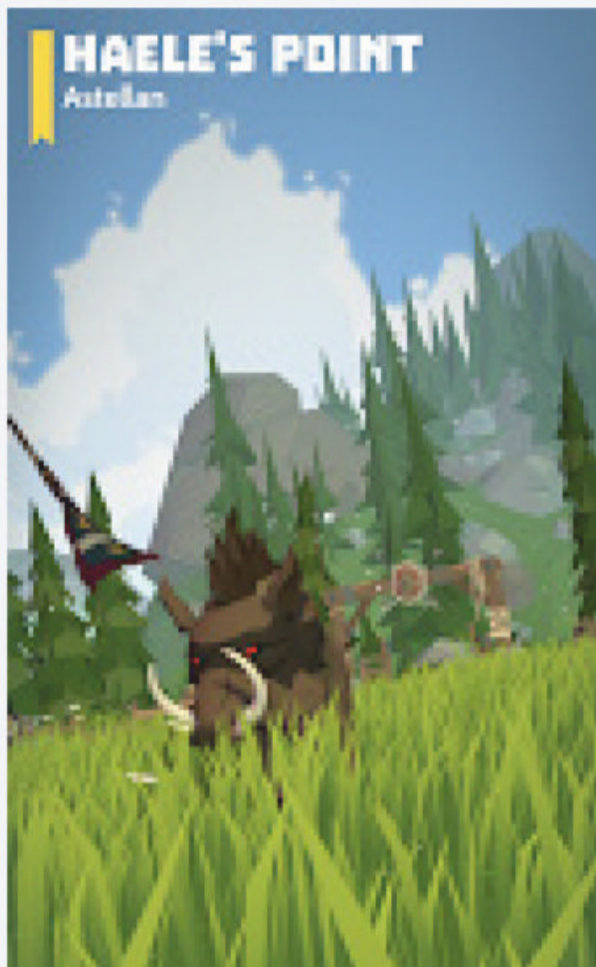Better than getting rucked in the face by a giant Welshman, but not by much.
Ben Wilson **TL**

# Mobile games

James Pinnell reviews the latest games for android & iOS smartphones & tablets.



## Knighthood
Free with IAP

Developer King has been famous for building applications like *Candy Crush*, but recently has attempted to broaden its appeal by creating experiences that cover adventure or action themes mixed with a little bit of puzzle. *Knighthood* continues this evolution by building an RPG with fixed levels but introduces a new style of combat – utilising taps and swipes from a third person perspective, mixing a turn-based battle system with one handed controls.

You can customise and upgrade your character with equipment you either pickup or unlock from chests, as well as team up with heroes that feature a skillset or element that exploits a weakness in battle. There are guilds, events, and team battles that allow friends and groups to focus their

strategies to take down larger bosses, and like most King games, the presentation and polish is slick and fast.

Unfortunately, it's also shallow over the longer term. Quite a lot of the higher levels introduce a difficulty curve that's linked to equipment and requires that payment be made if you want to stay competitive in the PVP battles as well as some of the more advanced guild bosses. Additionally, it can also feel quite grindy, as much of the core battle system's depth just isn't there, and much of it involves high damage response rather than uniquely exploiting weaknesses in your enemy. ★★★★☆

## Dragon Quest: For The Stars
Free with IAP

In Japan, *Dragon Quest* is one of the most successful video game franchises of all time. Starting around the same time as the much more well-known *Final Fantasy* series of games, its focus on a strict adherence to traditional Japanese RPG gameplay, stories, and graphics has provided a remarkably consistent and impressive slate of games.

This title is admirable in its absolute, steadfast addiction to the core gameplay loop of its "full version" games – a strong story, timed, turn-based combat, and a clever, skill and magic focused combat strategy.

Choosing the correct set of attacks, which is also managed before battle by equipping the right gear or stripping skills from older items, can mean the difference between your team being wiped out or meeting the optional objectives that net the rarer and more elusive items.

Monetisation is very fair and its possible to unlock epic items without paying any money or sinking hours into constant grindy battles. ★★★★★

> **"**
> *You can customise and upgrade your character with equipment you either pickup or unlock from chests, as well as team up with heroes that feature a skillset or element that exploits a weakness in battle.*

## Scrabble GO
**Free with IAP**

The sheer irony of *Scrabble GO*'s existence is that it managed to be gazumped by another unaffiliated title, *Words with Friends*, that dominated the early mobile/Facebook game space. *Scrabble* did have an app early on, but unfortunately for them it was poorly designed, cost too much and didn't include many of the social features that made *WWF* so popular to begin with.

*Scrabble GO* attempts to re-write this history by introducing the core *Scrabble* experience, with all its rules and board layouts, with the whole hog of social features, powerups and multiplayer functionality that the original missed. What's there now is a significantly improved and slick *Scrabble* experience, complete with a focus on non-real time play, multiple boards and opponents, ladders and advanced scoring.

Ironically, however, there isn't a lot here that differentiates it from Words with Friends, which now has years of refinement and a variety of different game modes that exploit much of what Scrabble Go is trying to do now.

★★★★☆
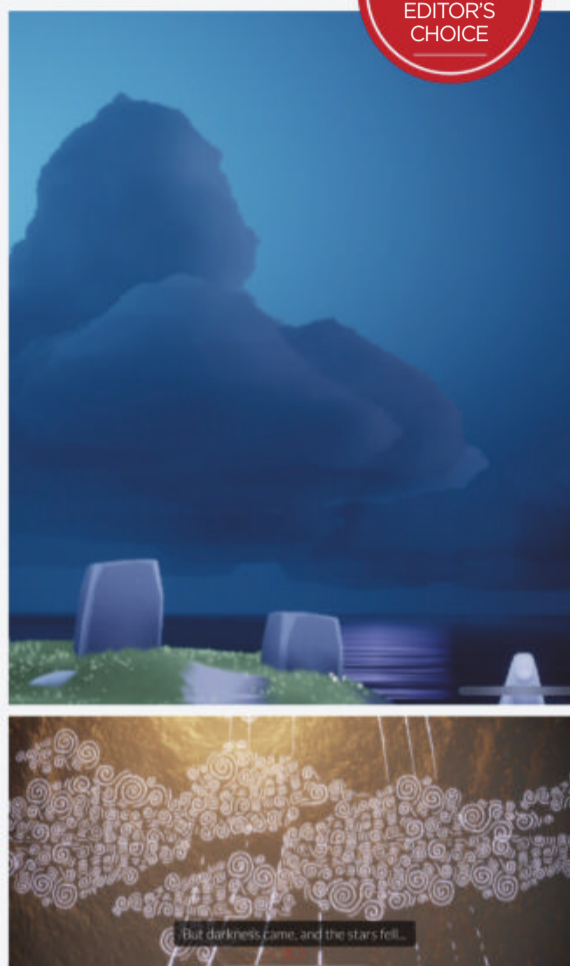
## Sky: Children of the Light
**Free**

*Sky* is one of those titles that absolutely needs to be played to be appreciated. It is a beautiful, soft and dreamlike experience across seven worlds that silently, effortlessly slides you into contacts with other players without any violent or exclusionary tactics. Much like the developer's 2013 smash, *Journey*, *Sky* allows you to play with others in a fashion that naturally establishes a sense of cooperation and shared experience. There's no lobbies, groups, clans or chat, just a smooth and ingenious method of natural flow that allows for a drop-in and out style of multiplayer exploration.

Playing *Sky* is effortless and beautiful – the controls are simple and easy to learn; the UI is minimalist and the sound quality is exceptional. I highly recommend you use some headphones when you play – every footstep, every movement, every new element and expansion of the world has its own soundtrack.

It's one of the better mobile adventures and you can't beat the price.

★★★★⯪

## Dragon Raja
**Free**

*Dragon Raja*'s unfortunate name will largely turn many people off, which is a shame due to the fact it is one of the most unique attempts at a mobile MMO in a long time, thanks to its heavy focus on a fully fleshed out and interesting story, along with very detailed and impressive cutscenes. It's rare that I bother paying attention to the shallow depth of plot lines within mobile games, but there was a distinct *Final Fantasy VIII* theme here I really enjoyed.

The other interesting aspect of this game is how it is structured – unlike most mobile MMOs, *Dragon Raja* is mostly a single player experience with some multiplayer actions tacked on. This doesn't always work, since the gameplay spins abruptly in and out of its single player mode without much clarity or context.

But where it does work – largely the dynamic and varied combat system – it becomes extremely moreish and addicting. There's a lot of character and class customisation too, which is a big plus for those who enjoy that type of RPG. ★★★★☆ **TL**

2020
TECHlife
EDITOR
APPROVED

$1,599, www.oppo.com

## Oppo Find X2

The Oppo Find X2 is the brand's new premium phone – and we like it.

When Oppo made its first concerted effort to break into non-Asian markets, it did so with the Oppo Find X in mid-2018, but since then it's found more success with the Oppo Reno series.

We'd heard rumors that Oppo was considering the return of the Find range, and a release date seemed likely for the end of 2020 – but then the company surprised us with a reveal of the Oppo Find X2 and Find X2 Pro at its MWC 2020 replacement event in early March.

The Oppo Find X2 is the company's first true premium device in two years (Oppo has told us that the aforementioned Reno devices, even the accomplished Reno 10x Zoom, which leads that pack, are now considered its mid-range series). It's clear that Oppo wants to make up for this lost time, and the Find X2 packs a smorgasbord of features that look seriously impressive on paper.

Specs on paper don't always translate into a great user experience in practice, though; so does the Oppo Find X2 have enough to rival phones from top-end competitors like Samsung, Apple or Sony? We got hands-on with the handset to find out.

### Design and display
If you were to combine all the features you associate with the phrase '2020 premium phone' and put them on one device, you'd have a phone very like the Oppo Find X2, although the design also incorporates some signature Oppo flourishes.

The 6.78-inch screen is curved at the edges at a 68-degree angle. The edges of the screen aren't quite as steep as Oppo's 'waterfall' screen that we've seen on concept devices before, but the curve certainly feels more pronounced in the hand than the edges on phones like the Samsung Galaxy S20.

> "The main snapper is joined by a 13MP telephoto camera that facilitates 5x hybrid zoom (combining optical and digital zoom) and then 20x digital zoom.

This display is broken up by a 'punch-hole' cut-out segment in the top-left corner. This did feel a bit intrusive to us, especially given that the original Find X had a pop-up segment for this camera.

When we asked Oppo about this, they told us they'd found that the pop-up mechanism took up too much internal space for just the front-facing camera, so we can see why the feature was dropped to make way for other tech inside this phone.

As was the case with the Find X, there's no 3.5mm headphone jack on the phone; unlike the Find X, Oppo told us the phone is IP54-resistant, providing partial dust and water splash resistance, but shy of the IP68 protection on the Pro version.

### Camera
On the back of the Oppo Find X2 you'll find a 48MP main camera, which would have been considered

pretty impressive in early 2019; in 2020, however, the best camera phones are pushing the limits to 64MP and even 108MP. Still, resolution isn't everything in a camera phone.

The main snapper is joined by a 13MP telephoto camera that facilitates 5x hybrid zoom (combining optical and digital zoom) and then 20x digital zoom. We weren't actually told the optical zoom limit of the device, but we'd estimate this at 2x based on the other zoom counts.

The third and final camera is a 12MP 'video lens' camera, with a 120-degree field of view (similar to that of an ultra-wide-angle lens).

## Features and specs

The phone runs on the top-end Snapdragon 865 chipset, which should deliver blazingly fast processing speeds, perhaps enough to rival the iPhone 11 or even the Samsung Galaxy S20.

This chipset comes with a built-in 5G modem, so the Oppo Find X2 is a 5G device, just like its

Find X2 Pro sibling; there's not going to be a 4G-only device, according to Oppo.

The Oppo Find X2 runs Android 10, the latest version of Google's operating system, with Oppo's ColorOS 7 laid over the top. This brings mainly aesthetic and navigation changes from stock Android, but we found the top-end screen tech really brings out the vibrant colors of its icons and buttons.

## Final Thoughts

If your eyes have been growing wider and wider as you read this review, you should definitely keep your eyes on the Oppo Find X2. Although we only got to test it out briefly, our experience was broadly in line with our expectations based on the top-end specs inside the phone.

One aspect we're a little dubious about though is the cameras. Most new smartphones, especially premium ones, are constantly pushing the limits of camera capabilities, with high-res

sensors, fantastic zoom performance, and a slew of impressive post-processing abilities; but Oppo seems to have brushed over the cameras in the Find X2 in favor of other features.

That said, we're looking forward to spending a lot more time with the Find X2, along with the rest of the phones features; it's possible that the snappers are better than the specs list gives them credit for. Likewise it's possible the top-end screen quality and fast charging speeds have unforeseeable negative consequences.

Time will tell, but so far, Oppo's onto something good.

★★★★☆

Oppo has packed its new flagship full of all the top-end features you'd expect from a premium device in 2020, and more, so there's certainly a lot to like here. The cameras do feel a little sub-par though, at least in terms of specs.

Tom Bedford

$2,399, www.asus.com

# Asus ZenBook Flip 15

A capable and premium 2-in-1 laptop.

The exquisite brushed metal – US Military grade quality, allegedly – aesthetic makes a big impact as soon as you take the Asus ZenBook Flip out of the box.

The material makes for a solid machine, and its finish provides a subtle design aesthetic that is both sleek, and makes a nice change from the basic black and silver designs we often see in modern laptops.

This design aesthetic makes the Asus ZenBook Flip 15 one of the nicest laptops we've ever used. It feels very robust too; teamed with a decent weight the ZenBook Flip 15 feels like it could survive a knock or two – although we'd never want to risk denting that beautiful brushed metal.

The design houses a glorious 4K screen with an impressive 90% screen-to-body ratio. This is thanks to the ultra-thin 4.5mm bezels that surround the display and help maximise the amount of screen the laptop packs into its chassis. It's impressive stuff.

Seriously, the screen is glorious, and made us genuinely gasp upon opening the laptop for the first time. The 'other' screen that's key in the laptop's design is that of the touchpad-meets-screen feature: the ScreenPad.

Above the ScreenPad is a keyboard that is stacked; it's a full keyboard with a numpad to the right too. That's quite the achievement on a 15-inch laptop. However, there's a compromise to be made for getting a full keyboard and numpad and ScreenPad into the laptop: everything feels a little cramped.

## Performance

The Zenbook Flip 15 tries to give you everything plus its own toys which means there's a competition for space – we found it was easy to miss keys or hit the wrong ones.

Unsurprisingly, the Asus ZenBook Flip 15 is a high-performing 2-in-1 laptop. Whatever we use the machine for, it handles it; however we use the machine, it works and performs. And, genuinely, our criticisms are few and far between.

One of them, however, does reside in the layout of the keyboard. Because it's so cramped, particularly toward the top rows of keys and the right hand side with the numpad, it is quite easy to smash the wrong button or flick the wrong keys to interrupt functions. The delete key, for example, proves very easy to miss. Also, the power button is a little too indistinct and the actuation is poor, too.

It's also a bit of a shame that there's no Ethernet port, but to be fair the ZenBook Flip 15 does counter that with very strong

> *Unsurprisingly, the Asus ZenBook Flip 15 is a high-performing 2-in-1 laptop. Whatever we use the machine for, it handles it; however we use the machine, it works and performs.*

and reliable Wi-Fi connectivity and strong Bluetooth 5.0 support, the latter being a particularly solid and welcome addition.

The screen is a true joy to use, without fault. It's a roomy, bright, crisp and clear display that is good for any function or task. Films and YouTube videos are vibrant and punchy; games are vivid, and even day-to-day software like Chrome and Microsoft Office look great. The 100% sRGB quality of the screen certainly helps with the top-notch image quality.

There is also something very satisfying in simply flitting between regular laptop touchpad and keyboard use, to scrolling down programs and opening up files by using the touchscreen itself, with only a lazy change of arm position.

Thanks to the powerful components within, daily use of the laptop, which included running multiple programs and apps at once, was incredibly smooth on the ZenBook Flip 15. It has more than enough grunt to handle everything that work or medium productivity such as photo editing, word processing, spreadsheet and web browsing all at once.

Meanwhile, the gaming benchmarks we ran reveal results that are both expected and pleasantly surprising.

They are not cripplingly slow, as you might expect from the aging graphics card housed in the laptop, but the Asus ZenBook Flip 15 also doesn't provide anything near a 'good' gaming experience.

Naturally, we ran benchmarks and played games at 1080p given it's a modest card, which would in no way handle the screen's native 4K resolution. However, the results do show you could still enjoy a bit of gaming on the go, albeit at lower settings and on with undemanding games.

The ScreenPad may seem like a gimmick, but it quickly became much more in our daily use.

> *You'll quickly embrace the ScreenPad with its built-in technology that supports smart gestures; you'll start to seamlessly rely on the IR camera's facial recognition to log you in with Windows Hello*

This ZenBook might not be a gaming laptop per se but it is a laptop that can play games... at a push. If only Asus had been able to work a 16-series card into this ZenBook then we would almost certainly have given it a higher overall score.

Away from the gaming performance, the ZenBook Flip 15 manages to feel so much more than the sum of its parts. While the components do a fine job of powering the laptop, it's the extra features that really make it stand out.

In fact, the more you use it, the more true this becomes, and things like the ScreenPad, which many will dismiss as simply a gimmick or curio, start making a lot more sense.

You'll quickly embrace the ScreenPad with its built-in technology that supports smart gestures; you'll start to seamlessly rely on the IR camera's facial recognition to log you in with Windows Hello; it'll slip easily into your wider smart home setup through its built-in Amazon Alexa functionality; and swapping between tablet and regular laptop modes soon becomes second nature.

These features, backed up by the quality components under the hood means the Asus ZenBook Flip 15 is an all-round quality machine. Everything about the laptop performs really well – even the speakers are pretty good! If you can stomach its slight drawbacks, you absolutely will not regret acquiring one of these beauties.

★★★★☆

A great do-it-all laptop that ticks a lot of boxes. It's a quality 2-in-1 device that will handle anything from work to light gaming, and features one of the best screens going on a portable machine.
Rob Dwiar

$1,699, www.samsung.com/au

# Samsung Galaxy Book S

Samsung's Galaxy Book S is thin – both in terms of form-factor and usability.

On paper, Samsung's Galaxy Book S comes across as a very attractive proposition – it's both impressively-thin (11.8mm) and ultra-lightweight (961g) for a clamshell notebook that runs Windows 10, making it seem like an ideal option for those who often take their work on the road. That said, the fact that it's powered by an ARM-based processor will undoubtedly present a number of performance and compatibility issues for those who want to do more on their machine than run productivity apps and browse the web.

From a design standpoint, there's no denying that the Galaxy Book S is gorgeous. Minimalism is the word of the day here, with the notebook's lid curving towards the hinge and sporting an anodised aluminium finish that's complemented by a small and shiny embossed Samsung logo. On the sides, it's got two USB Type-C ports (neither are Thunderbolt, unfortunately) and a 3.5mm headphone jack, so you'll have to

rely on dongles for anything else. Additionally, there's a microSD slot on the laptop's underside, giving users the option of expanding on the 256GB of storage that's already onboard.

When opened, the Galaxy Book S reveals a 1080p touch display (a surprising step down from the first Galaxy Book's 1440p screen) with minimal bezels along its top and side edges (and a significantly larger one below), along with a chiclet-style keyboard and decently-sized trackpad. The design is not without its flaws, though – the combination of a light body and stiff hinge make it extremely tricky to open the Galaxy Book S one-handed.

The Galaxy Book S's sleek design is made possible by the ARM-based Snapdragon 8cx processor that powers it. While it's essentially a beefed-up mobile chipset, it's able to run Windows 10 Home in a fairly snappy manner – and with the added bonus of built-in LTE connectivity. Regrettably, that same processor

We really would have liked to see a backlit keyboard.

is also the main source of the Galaxy Book S's shortcomings. For starters, it'll only run 32-bit applications, or those which have been ported over to ARM64. Because of this, we weren't even able to run the majority of our usual benchmark programs. Geekbench was one of the apps that did work, however. Our results were wildly inconsistent with what we've seen on a number of benchmarking websites – in our CPU benchmark tests, the Galaxy Book S achieved single/multi core scores of 2071/6461, placing it above last year's ARM-based HP Envy but well below the likes of Microsoft's Intel Core i5-powered Surface Laptop 3.

★★★½☆

Samsung's Galaxy Book S works fine as a secondary device for lightweight tasks – just don't expect too much more from it beyond that.

Stephen Lambrechts

$2,499, www.acer.com.au

# Acer Predator CG7

An epic screen.

At this price, the Acer Predator CG7 is certainly one of the more expensive gaming monitors you can buy right now – but then it's also one of the largest (apart from those 65-inch Nvidia Big Format Gaming Display (BFGD) monitors like the HP Omen X Emperium 65).

However, when compared to 43-inch 4K TVs, like the Panasonic GX800, it's also pretty pricey, and many 40-inch 4K TVs can be had for half the price, and offer comparable visual quality, including HDR support.

What these sets don't offer, however, is the high refresh rates and gaming-centric features of the Acer Predator CG7. So, it's clear that this is a monitor that's aimed at people who want to game on a large TV, while also benefiting from tech usually found in gaming monitors. That's a tricky – and niche – market to go for, and if you're not careful, you can end up appealing to no one.

The design of the Acer Predator CG7 is similar to what we've come to expect from Acer's Predator

lineup of gaming peripherals, so you get some rather angular corners and RGB lighting that leaves you in no doubt that this is a product aimed at gamers. One rather nice touch is the icons on the stand that encourage you to store your game controllers there. The RGB lighting can be configured with preset lighting patterns, or set up to sync to your music and games..

Port-wise, the Acer Predator CG7 comes with three HDMI ports, two DisplayPorts, a USB Type-C port, four standard USB ports (two 2.0 and two 3.0) and a USB input, allowing you to turn the monitor into a USB hub. That's a good selection of ports, though it doesn't come with a TV tuner. That means, if you want to use the Acer Predator CG7 as a TV – and considering its size, you probably will – then you'll need to plug in a separate set-top box.

When it comes to performance, the Acer Predator CG7 is an impressive beast – though there'd have to be something seriously

wrong if it wasn't at this size. Plugging it into our test machine, Windows 10 discovered and configured itself accordingly, though we did have to pop into the settings to find a level of scaling that works best considering the size of the screen.

The Acer Predator CG7 has HDR (High Dynamic Range) support in the form of VESA DisplayHDR 1000. This is a high-end implementation of VESA DisplayHDR which has a peak luminance of 1,000 cd/m2. While it's not up to the standard of high-end TVs that have HDR10+ and Dolby Vision, it's one of the better implementations of VESA DisplayHDR – and the fact that it has a very bright peak luminance means it's capable of vibrant images.
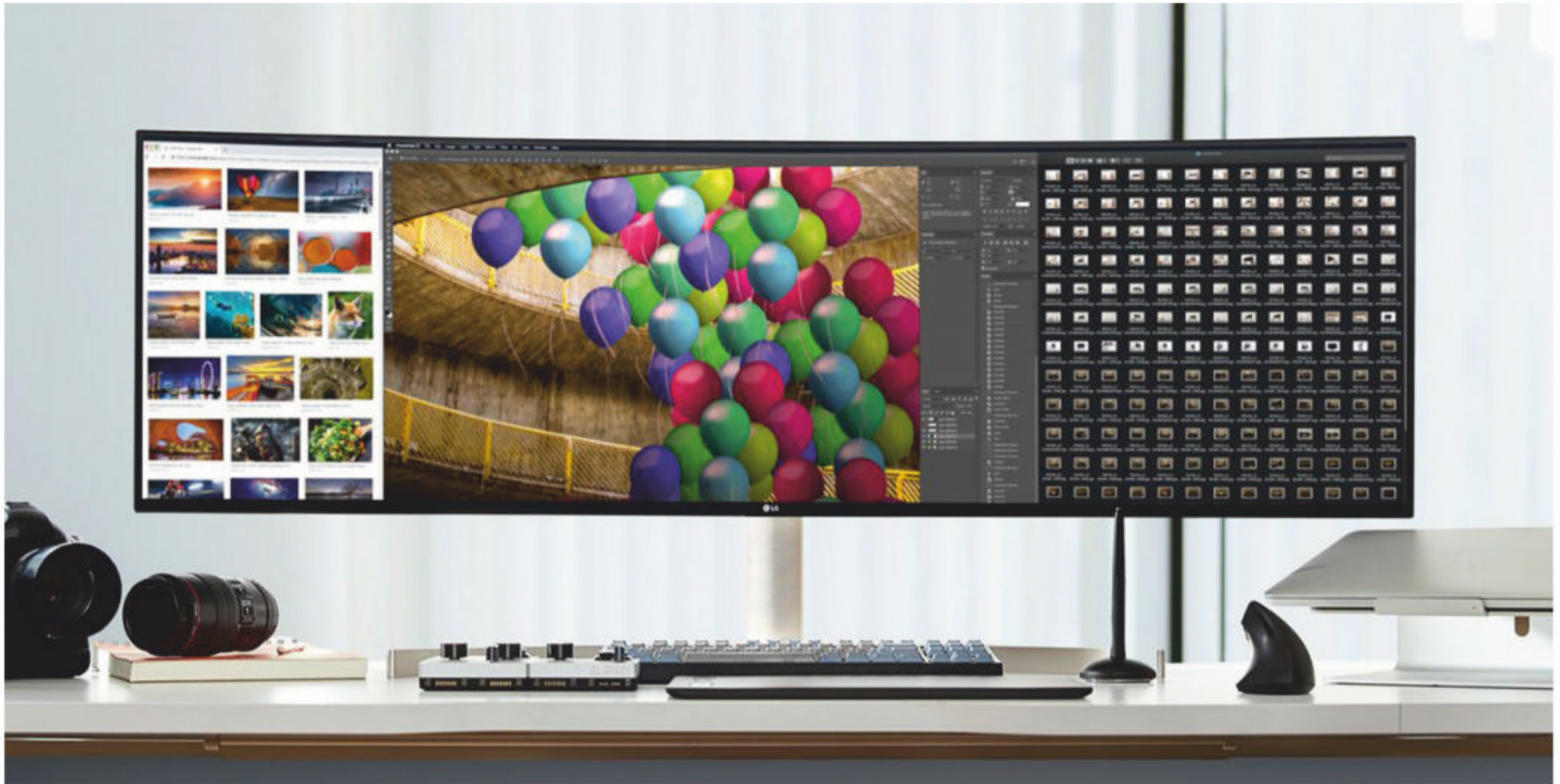
★★★★☆

The Acer Predator CG7 is a huge gaming monitor that brings certain features we'd expect to see in a gaming monitor to a TV-sized screen.
Matt Hanson

$1,899, www.lg.com

# LG 49WL95C

The LG 49WL95C is a huge monitor – but is it any good?

We've seen it all before here on TechLife, but the sheer size and scale of the new LG 49WL95C ultrawide monitor still blows our tiny minds.

The full 49-inch diagonal of the curved LCD panel is impressive enough on its own. But it's the 32:9 aspect ratio that makes this monitor so incredibly eye popping. It's just so wide.

Stunning the LG 49WL95C most certainly is, therefore. But does that actually make for a usable, practical and enjoyable display? Given the $1,899 price tag, it had better. It's also worth noting that the LG 49WL95C is not alone in the market. The Philips Briliiance 499P9H, for instance, matches it in most significant regards and undercuts it substantially on price.

Anyway, as with that Philips display, the biggie in literal and figurative terms here is the 5,120 by 1,440 native resolution. In most contexts, that would be a lot of pixels. On a 49-inch panel? Not quite so much. It's actually fewer pixels overall than a conventional 4K or UHD monitor. It also makes for a somewhat underwhelming 109 pixels per inch.

Overall, the LG 49WL95C feels very generous in its horizontal aspect. It's physically very wide and the 5,120 horizontal pixels provide plenty of space to arrange multiple apps and windows. Vertically, it's less impressive. The 1,440 vertical pixels fall well short of the 2,160 of a 4K monitor and leave you feeling slightly constrained.

At this price point, we'd be happier with the full 4K vertical resolution and then a boosted horizontal pixel count to suit, which in this case would work out to 7,680. That would also improve the pixel density and sharpness.

Anyway, that aside the image quality is strong but not spectacular. LG has specified a decent IPS panel with good colours and viewing angles. But it's not a particularly high fidelity. For starters, it only covers 79% of the Adobe RGB colour space and 99% of sRGB. Not bad figures, per se,



A good IPS panel doesn't quite make up for a low pixel density.

but not the stuff of demanding content creation either.

Similarly, while the LG 49WL95C is HDR10 compliant, with a peak brightness of 350cd/m2 and no local dimming, this is a monitor that can process HDR content but can't really display HDR visuals.

As for gaming, you'll need a hefty graphics card to drive the LG 49WL95C smoothly. Even then it's limited to 60Hz, which isn't ideal for shooters. Immersive it certainly is, and the sound quality from the built-in speakers is actually pretty tolerable. But the LG 49WL95C is not intended to be an out-and-out gaming panel.

★★★☆☆

The 49WL95C 32:9 aspect 49-inch ultrawide monitor is a feast for the eyes and full of features, but makes a major assault on your wallet.
Jeremy Laird

> *The YAS-209 supports lossy Dolby Digital, Dolby Pro Logic II, and DTS Digital Surround, but also includes DTS Virtual:X.*

2020 TECHlife EDITOR APPROVED

$345, au.yamaha.com

# Yamaha YAS-209

An affordable virtuoso sonic performer.

The Yamaha YAS-209 is an exercise in minimalism, with curved edges and a wrap-around black fabric grille. The top is also matte black, so no danger of annoying reflections from the TV screen. The build quality is good and the design will pair well with TVs that are between 55 to 65 inches. There's also a choice between stand or wall mounting..

This minimalism extends to the display, which is simply a series of small LEDs on the top panel. These LEDs register which input you have selected – HDMI, TV (ARC), Bluetooth and Net – along with indicators to show if the surround mode or clear voice has been selected.

To the right of these indicators, you'll find some basic touch-sensitive controls for source selection, volume up/down, and power on/off. Thanks to Alexa now being built-in, there's also a button to wake it up and another to mute the far-field microphones, two of which are located above the indicators and controls.

The YAS-209 supports lossy Dolby Digital, Dolby Pro Logic II, and DTS Digital Surround, but also includes DTS Virtual:X. This is described as 3D surround sound processing for a single soundbar solution, which basically means it uses psychoacoustic processing to create the illusion of more than its 2.1 channels.

The Yamaha YAS-209 is exceptionally easy to setup – simply place it under your TV or wall mount it using the rear screw holes and provided template. The subwoofer is best positioned at the front of the room, either to the left or right of the soundbar (whichever is convenient). Then all you need to do is connect your sources using HDMI, optical digital or Bluetooth.

The HDMI connections offer the best sound quality and the greatest convenience. Despite there being an HDMI input, you can simply connect all the HDMI sources to your TV and then send the audio back via ARC (audio return channel).



The lack of MusicCast is disappointing but ultimately forgivable at this price.

You can connect the Yamaha to your network using either a wired or wireless connection. For the latter you will need to use the Soundbar Controller app. The process is very easy, and you should be up and running in no time. Once that's done you can setup Amazon Alexa.

As a smart speaker, this soundbar proves surprisingly effective. The built-in far-field microphones are suitably sensitive, allowing for seamless interaction with Alexa. The smart assistant is clear and precise when answering questions, and the ability to easily stream music is a great feature. There's even limited voice control, which is useful when the remote isn't to hand.

★★★★☆

The Yamaha YAS-209 is a well-designed soundbar and subwoofer combination that produces as surprisingly big sonic presence, and thanks to Amazon Alexa it also doubles as a fully-functioning smart speaker.
Stephen Withers

$249.99, epson.com

# Epson Expression Photo XP-8600

A high-quality photo printer with an equally high price.

There are plenty of affordable multi-function printers that can provide good quality text and graphics for home and office users, but Epson's new XP-8600 is a specialist printer that is very much aimed at keen photographers who want to produce really high-quality photo prints.

It's a bit pricey, costing $249.99, but that price includes a six-color printing system (rather than the four colored inks used by conventional inkjet printers) that produces more subtle color graduations and lifelike skin tones for portrait photography. It's packed with useful features too, including Wi-Fi and USB connectivity, support for AirPrint for iOS devices, and two-sided printing. There are two paper trays that hold 100 sheets of A4 paper, and 20 sheets of photo paper. You can print on CD and DVD disks, and there's a third tray at the back for special art papers and cards, so the XP-8600 can handle just about every printing task you throw at it. And, of course, it also features a scanner and copier.

Print speed for text and graphics is fairly modest, at around 8.5 pages per minute, but the XP-8600 zips along when it comes to photos, taking just 18 seconds to produce a four-inch by six-inch photo print. The quality is impressive too, with the six-color printing and 5760x1440 dpi resolution producing finely detailed photo output, with bold colors and strong contrast. But replacing six separate inks can be expensive, so the XP-8600 will only be suitable for keen photographers who are prepared to pay for that extra quality.

★★★★☆
Expensive, but the quality six-color photo printing is worth it for serious photographers. Jennifer Allen

$149,  en.rode.com

# Rode NT-USB Mini

Compact, rugged, and simple USB audio recording.

While the Blue Yeti and its more compact Nano successor have been the go-to for many seeking budget USB microphones, Rode is hoping its latest NT-USB Mini will steal their thunder.

The interface on this little Rode mic is incredibly tidy, with a USB-C and 3.5mm headphone ports found on the rear, and a single dial found on the front that adjusts headphone level when turned and enables monitoring when pressed. It features an integrated pop filter and is constructed from hard-wearing steel and reinforced nylon resin, so it's compact and rugged enough for grab-and-go situations. The desktop stand is attached magnetically and weighted to absorb any shocks from a bumped desk, while the swivel mount can be easily detached and mounted on a mic stand or boom arm. The NT-USB Mini is class-compliant, meaning it will work immediately with any computer or tablet when hooked up via USB, with no drivers, firmware or apps required. We found the audio recorded with this Rode mic to be exceptional given its size and pricing, but as the website suggests, a distance of 10-15cm from the sound source is optimal to reduce background noise. This can be problematic given its diminutive size when attached to the provided desktop stand (a problem it shares with its primary competitor, mind you) as you'll often need to lean in or talk at your desk.

★★★★☆
Minor gripes aside, the NT-USB Mini is an excellent offering for podcasters, streamers, and casual musicians alike, providing solid audio in a simple, rugged package at a price that's hard to fault.
Harry Domanski

$749, www.insta360.com

# Insta360 One R

Is this modular action camera the best of all worlds?

The One R is a truly modular action cam – one third is battery, another block is home to the controls and screen, while the last part is the lens and sensor brick.

This style lets you choose one of three cameras to slot into the Insta360 One R – there's a 4K action camera, similar to the GoPro Hero 8 Black, and the 360-degree camera is nearer to the GoPro Max.

We had two initial concerns about the Insta360 One R. Would the modular design make it huge? And would feel as if it was always about to fall apart?

Both of these were unfounded. The Insta360 One R is only a bit bigger than a GoPro Hero 8 Black, and is surprisingly sturdy.

There's no tough locking mechanism to keep the control block and camera lens part together, but the One R feels rigid enough when you clip the battery base in at the bottom. Sure, the Hero 8 Black looks more accomplished, and its soft touch finish feels better too. But Insta360

has managed to make the modular design here seem almost practical, rather than a strange science experiment.

When you want to switch lenses, you simply unclip the battery, pull the lens off and slot in your other module. It takes around 20 seconds.

The Insta360 One R's screen introduces our second issue. It's a 1.3-inch square display, similar to the front screen of the DJI Osmo Action.

You use this to compose your shots and navigate the interface. And this is a lot to ask of such a tiny touch display.

Shoot a 16:9 aspect video and the preview becomes even smaller. There was no comparison, using it side-by-side with the Hero 8 Black. The GoPro screen is far more comfortable to operate, and is no user experience revelation itself.

The Insta360 One R dream is standard 4K video capture that can match the GoPro Hero 8 Black and 360-footage that



Software issues make the Insta360 One R less than user-friendly

rivals the GoPro Max. We are a way off that dream, but there are several things to like here. Let's start with the 4K wide-angle camera, which is the 'normal' side of the One R.

We went out to the park for a run to shoot side-by-side with the Hero 8 Black and One R. The sharpness and of the stabilisation, which Insta360 calls FlowState, are roughly similar. Both are great and the One R captures a lot of detail at 4K resolution in good lighting.

The Insta360 One R succeeds in areas that it could easily have failed in, coming from a company that fires out dynamic action camera designs at quite a rate. But it also trips up in predictable ways, particularly when compared to the more polished alternatives from GoPro.

★★★★☆

The Insta360 One R is a unique action camera that offers comparatively good value when compared to non-modular rivals like the GoPro Hero 8 Black and GoPro Max.
Andrew Williams

2020
TECHlife
EDITOR'S
CHOICE

$599, amazon.com

# DJI Mavic Mini

An ultra-small, ultra-light affordable drone.

DJI's latest addition to its fleet is aimed at bringing drones to the masses, thanks to a lower price and a tiny weight of 0.5lb.

That weight includes the battery and microSD card (32GB included). Like bigger Mavic drones, it's foldable, so it becomes dinky enough to carry around with ease at just 6.3 inches long, eight inches wide and 2.2 inches tall.

The Mavic Mini shoots 1080p video at up to 60fps and super-crisp 2.7K at up to 30fps. The fact that it doesn't shoot in full 4K is no real hindrance since this drone isn't aimed at pro video work – what it takes looks fantastic on a tablet or phone.

For those who are into aerial photography, the drone's camera shoots immaculate 12MP stills that really "pop" when snapped in good lighting conditions. It isn't too shabby in low light either.

Despite its diminutive dimensions, the Mavic Mini is extraordinarily stable in flight and very fast and nimble when switched to Sport mode, while a reliable GPS lock keeps it stationary when it's not moving. On the automative flight mode front it offers a small variety of "Quick Shots" including dronie, rocket, circle and helix, but no follow-me mode.

Unlike some other drone controllers, the DJI Mavic Mini's doesn't include a screen; instead it unfolds to hold an Android or iOS smartphone. Tucked away in its body are screw-on joysticks, so that when it's collapsed the controller has a flat profile, and when opened out it delivers a traditional feel.

On the left side of the controller is a micro USB port for charging and connecting it to your phone. The drone also ships with Lightning, micro USB, and USB-C cables, so whatever smartphone you have, provided its software is compatible with the DJI Mavic Mini's Fly app, you're catered for.

The controller's jog-dial at the top pivots the camera vertically through 90 degrees,



The Mavic Mini folds up into a conveniently small size for carrying.

so it can look forward through to down. Unlike the Anafi, it can't look up, which would have been a bonus, but its range is typical of most drones. Buttons of note include the L trigger, which starts video recording, and the R trigger, which takes a photo – perfect if you're operating the drone while wearing gloves.

Nothing else this size does what the Mavic Mini does, and when you look at the competition our wish list is easy to ignore. The Mavic Mini is DJI's lightest, most affordable drone to date, is an industry leader in terms of portability and performance, it delivers impressive 30-minute battery life, with most sub-250g drones dying after 10-15 minutes.

★★★★★

Incredible value and ultra-compact size. Flies impeccably. Shoots superb video and takes great images. No obstacle avoidance or follow-me mode.
Derek Adams + Basil Kronfli

$499.95, www.sennheiser.com.au

# Sennheiser Momentum True Wireless 2

Sennheiser could have a winner on its hands.

The new true wireless earbuds look pretty similar to their predecessors, the Sennheiser Momentum True Wireless, with shiny touch-sensitive housings, and a rounded shape; their metallic finish looks slick and stylish, without being overly ostentatious.

The charging case has a similarly sophisticated look, with a gray fabric finish; on the back you'll find a USB-C charging port, and a small button that you can press to see how much battery the case has via a little LED that glows red, orange, or green.

If your ears are on the smaller side (like ours), you may find that the circular housings feel a little uncomfortable; they're quite unwieldy, and after a longer listening session our ears felt quite sore. In fact, it almost felt as though the housings of the earbuds were cutting into the surrounding skin.

If you do find the fit to be comfortable, you should be able to use the Sennheiser Momentum

True Wireless 2 for as running earbuds, as they come with an IPX4 and therefore should be able to resist a little sweat or a few drops of rain.

Pairing the Sennheiser Momentum True Wireless 2 with our smartphone was seamless thanks to support for the latest wireless streaming standard, Bluetooth 5.1.

These buds also boast a much longer battery life than their predecessors, with seven hours from the buds themselves, and a further 21 hours from the charging case. That's up from four hours in the earbuds, and eight from the charging case, putting them on a par with the best true wireless earbuds of 2020.

Aside from better battery, the big selling point of the Momentum True Wireless 2 is the addition of active noise cancelation. We found that, while these buds block out some environmental noise, a fair amount was able to leak through – turn your music on though, and the rest of the world will melt away.



Not ideal for those with smaller ears, but near perfect for everyone else.

Like their predecessors, the Momentum True Wireless 2 are packing 7mm dynamic drivers, which the company says will create "outstanding stereo sound, with deep bass, natural mids, and clear, detailed treble".

These buds don't boast the widest soundstage we've ever heard, but they don't sound too closed off, either – and they provide plenty of crisp detail. When it comes to sound quality, battery life, and connectivity, we're very impressed with the Sennheiser Momentum True Wireless 2 so far. They represent a true upgrade over the original buds, and could even give the Sony WF-1000XM3 a run for their money in terms of sonic prowess.

★★★★☆

The Sennheiser Momentum True Wireless 2 are a real upgrade on the original earbuds, with good noise cancelation, better battery life, and excellent sound quality. It's just a shame they won't fit all ears comfortably.
Olivia Tambini

# BARGAIN HUNTER

The best free video-editing software

## Lightworks

Free, www.lwks.com

Lightworks is the best free video editor for anyone who wants to create professional-quality movies and videos without paying a penny. It supports multitrack video and is a non-linear editor, so the quality of your footage won't be affected by processing.

With Lightworks, you'll find all sorts of high-end features that are normally only available with expensive packages such as Final Cut Pro. These include the ability to import and render footage in the background, and to preview video effects in real time.

You can drag various editing windows around to create an almost infinite number of layout variations and set custom keyboard shortcuts to speed up your editing jobs.

You can download and install Lightworks for free, but if you decide you want to invest in an improved experience, you can upgrade to Lightworks Pro. ★★★★★

## Hitfilm Express

Free, www.fwwxhome.com

Hitfilm Express is a free-to-use video editor that aims to make a professional editing experience available to everyone. With this software package, it's easy to adjust color balance, trim clips, and export your projects in different video formats.

But the Hitfilm Express feature set goes way beyond that. You can also use this free video editor to set green screen chroma keys, create custom video masks, and take your footage to the next level with a range of 3D compositional tools. Although first-time users may find it a little confusing, the HitFilm Express user-interface will be familiar to anyone who's worked with an advanced video editor before.

There is a small downside to using this video editor, however: the installation process is unnecessarily complex. To get access to the Hitfilm Express software, you'll need to share a link to its developer, FXhome, on social media.

★★★★✫

# Shotcut

Free, www.shotcut.org

A rather unusual development journey has resulted in a slightly odd–looking user interface for this app, but Shotcut is still one of the best free video editors you can download now. Some aspects of the Shotcut editing system are easy and intuitive, such as the process of dragging media files to import them into your project. However, there's no doubt that there's a steeper learning curve with this video editing software than most. For example, you'll have to configure your display by adding the modules you need.
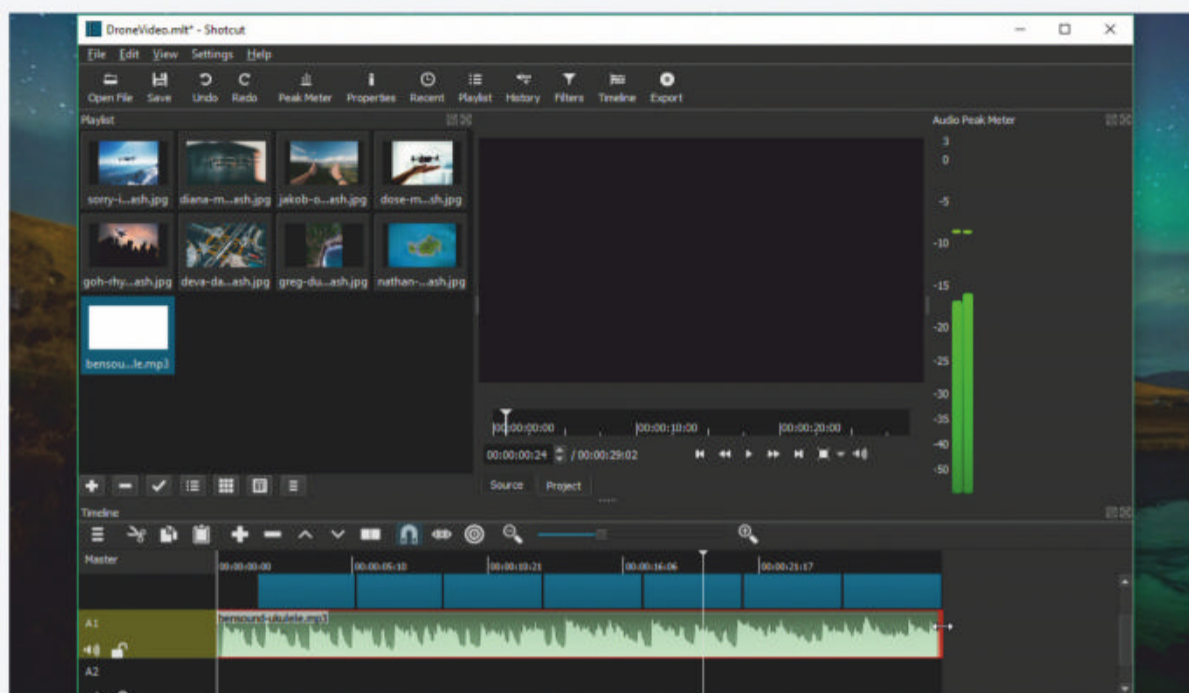
But once you get the hang of Shotcut, you'll discover why this free video editor has amassed such a large following.

The best Shotcut feature is a large selection of filters that can be applied to audio and video content. Once added, you can layer and customise filters to achieve the precise effect you're looking for.

★★★★☆



Movie Maker Online uses an unusual vertical project timeline.

# Movie Maker Online

Free, www.moviemakeronline.com

Movie Maker Online is a video editor that runs in your browser. To edit a video, you simply need to upload it before you can crop clips and add filters or transition effects. Other free video editors listed here are software packages that can be installed and run locally. However, the big advantage of an online editor is that you can access it from any desktop device, and there's no need to worry about content storage. Another big bonus is that your computer specs don't matter as much, the age of your hardware doesn't matter when using an online video editor as everything happens in the cloud.
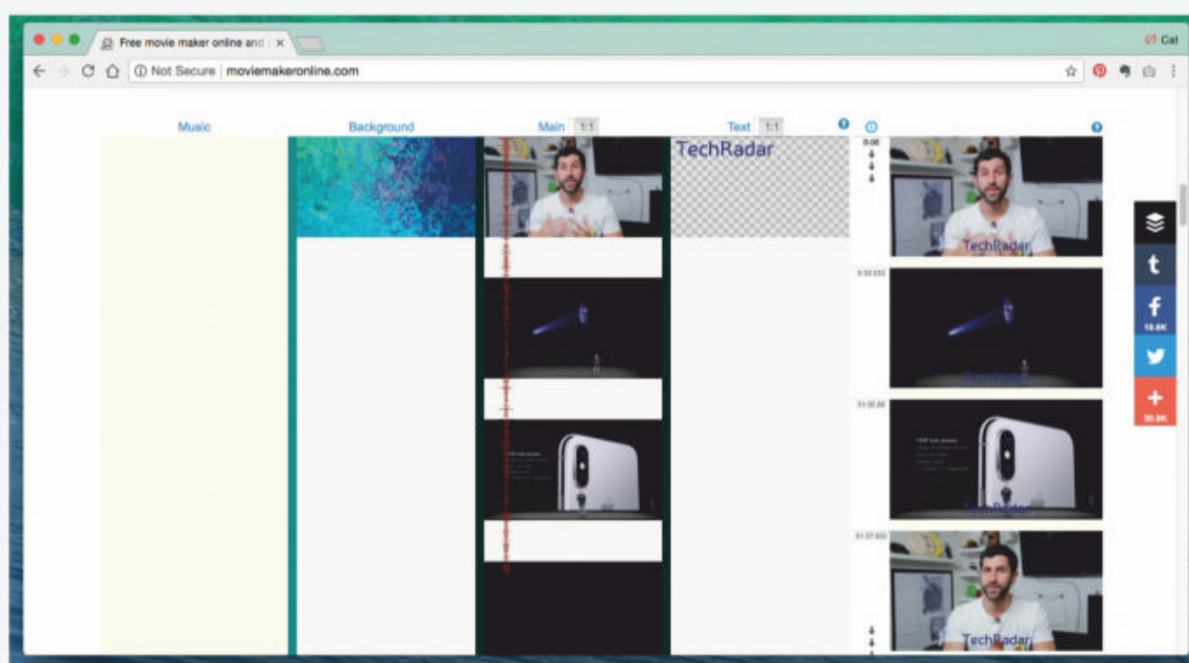
If you want to enhance your video or movie with music or still images, Movie Maker Online has a large archive of royalty–free images that can be inserted into your timeline with a single click.

★★★½☆

# KEEP YOUR LAPTOP SECURE!

# SEEK AND DESTROY
# MALWARE

Discover how to protect your PC from malware, plus how to get rid of any infections that sneak through.

Unless you've lived under a rock your whole life, you'll have come across malware at some point, whether it came to you via floppy disk or a dodgy website. The question remains, how do you protect yourself against it, and what can you do should you find your PC infected? In this feature we'll answer these – and other – questions.

We'll open with a quick run-through of the most common forms of malware you're likely to encounter, from traditional worms and Trojans to backdoors, rootkits and ransomware. We'll then help you perform a security audit of your PC – you'll find Windows 10 is much better at protecting you than earlier versions of Windows, but there's still room for improvement.

Then it's on to the tricky question: what do you do when an infection sneaks through your defences? We'll step you through the techniques and tools you'll need to not only wrest control of your computer back from whatever malware has invaded it, but also start to clean up the mess it leaves behind.

These days you're under threat online too – we'll finish by taking a look at ways you can avoid being targeted when using the internet, boosting privacy and security and making the web and other online activities a safer, more pleasurable experience once again.

# Threats to your PC's security

Receive a complete rundown of the key dangers – malware, hackers and more – that threaten your PC.

Threats to your privacy and security come in many shapes and forms these days. Let's start by taking a brief tour of the different types of malware around to provide you with a better understanding of what to look out for.

## Virus/worm

Traditionally malware was conflated with the term 'virus'. However, viruses are a specific form of malware: code inserted into other files (such as macros in Microsoft Office documents, which is why macro supported is now disabled by default in Office). Along with worms – standalone programs rather than malicious code hidden inside other files, viruses are primarily a mechanism for delivering so-called malicious 'payloads', and are designed to replicate themselves as far and wide as possible, such as through copying to shared network folders or hiding inside emails.

## Trojan horses

These days, a more common form of malware comes under the 'Trojan horse' heading. As the name suggests, they're called Trojans because they attempt to sneak on to your PC under false pretences, typically by masquerading as

legitimate software. Once installed, they can deliver different kinds of payloads, from changing system settings to prevent you from detecting and removing the threat to spying on your activities and downloading more malware to your PC.

## Zero-day exploits

The never-ending release of security updates for Windows, web browsers and other software are a constant reminder that security holes are constantly being discovered – these holes make it possible for hackers to inject malware or take control of compromised systems using zero-day exploits. The 'zero day' is a reference to the time it takes between



Malware comes in all shapes and sizes, with some Trojans more dangerous than others. Windows Security provides ratings for each.

discovering a hole and patching it. People's reluctance to install security updates, thus increasing the risk from zero-day exploits, is one of the reasons why Windows 10 makes such updates mandatory.

Zero-day exploits can carry all kinds of malware payloads, and your best bet for protecting yourself in the interim
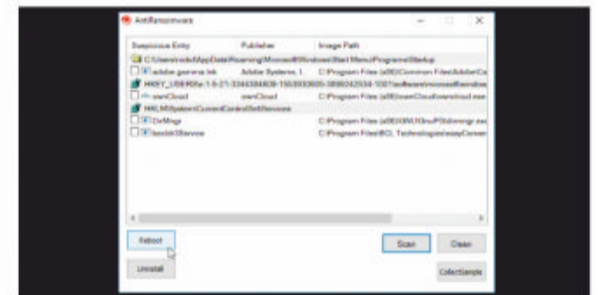


Dedicated anti-ransomware tools are available, but the trick is obviously to avoid ever being infected.

# POTENTIALLY UNWANTED PROGRAMS

One grey area when it comes to malware is that related to Potentially Unwanted Programs, or PUPs. Some application installers offer you additional programs, toolbars and other software during the set-up process – most are perfectly legitimate, but there are question marks over the practice. This so-called 'bundleware' is used to help fund development of programs, ensuring they remain free of charge, but the practice can be abused. Most PUPs are harmless – and definitely not malware – but some can harbour spyware, browser hijackers and other unwanted programs. The major problem is that they're often pre-selected for installation by default, and the terminology for rejecting the offer can be confusing. What exacerbates the problem is that most security software ignores program installers that offer PUPs as they technically require your authorisation – however poorly framed – before they can be installed. Two programs that can help keep PUPs off your PC are the premium version of Malwarebytes Anti-Malware (see over the page) and a free program called Unchecky (**www.unchecky.com)**, which we recommend for all users.
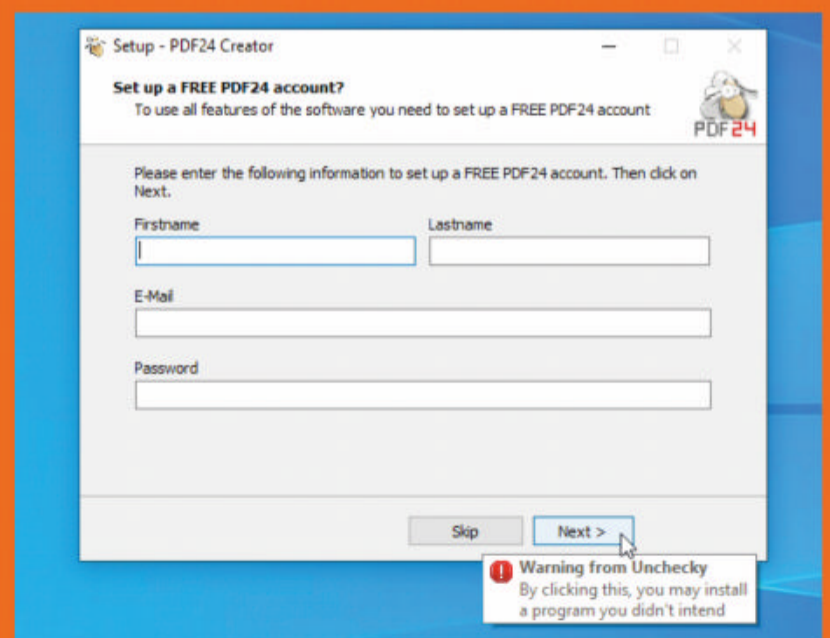


Unchecky is a tool that can detect (and deselect) some PUP install options, plus it will warn you about others.

between discovery and patching is to ensure your security software has built-in protection against them using heuristics, which acts on suspicious behaviour that may indicate the presence of malware.

## Backdoor

An infection that allows hackers – typically automated scripts or other infected computers (known as zombies or 'bots') to remotely access and control your PC. Delivered by worms and Trojans, they can do anything from use your computer to deliver spam, steal personal information or act in conjunction with other infected PCs (collectively known as 'botnets') to attack major online services through Distributed Denial of Service (DDoS) attacks.

## Spyware

While traditional viruses aim to replicate themselves far and wide, spyware tends to exclusively focus on the computer it's been installed on. Its primary aim is typically to collect information about you – through spying on your usage – often to target you with ads and other material for financial gain. It's also often used to steal sensitive information such as financial data and passwords through the use of a keylogger, which monitors keystrokes and mouse movement.
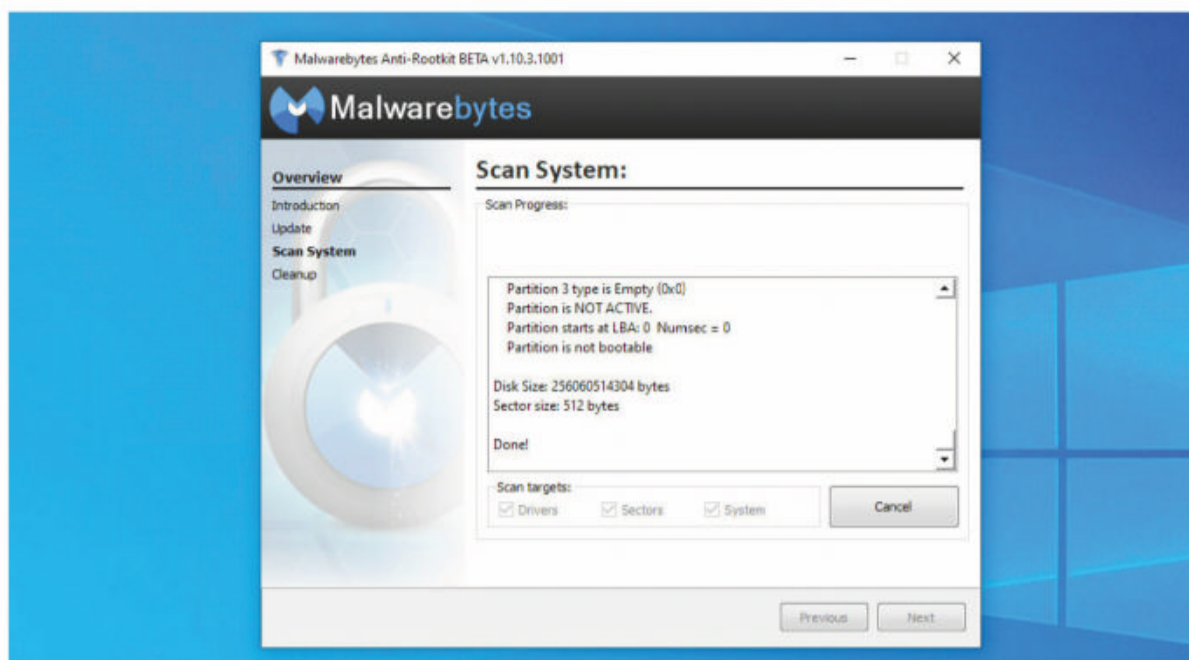


Dedicated tools for removing rootkits exist from several vendors – Malwarebytes' version has been in beta for years, and is free to download from **www.malwarebytes.com/antirootkit/**

Like other forms of malware, spyware also attempts to change computer settings – particularly internet-based settings. This is to both protect itself by making it impossible to visit security-based websites, plus make use of whatever information it's gathered.

## Rootkits and ransomware

Rootkits are a special form of malware that's designed to conceal its own presence – in the form of tell-tale processes and running programs – and actively protect itself from being removed by security software. Thus hidden, the rootkit can then introduce payloads that can steal user information or even hijack the computer for use as part of a larger botnet network.

Ransomware is even more insidious. It seizes control of your PC and demands you pay to restore control (or decrypt personal data). It's delivered in many different ways, from regular infections and other vulnerabilities (such as backdoors) to phishing – tricking users into running programs. Unlike other malware, it makes no attempt to hide.

Once triggered, you're either locked out of your entire PC or key parts of the system, and you may find all personal files are encrypted, spreading to any connected network shares and backup drives. You'll receive regular prompts – and a deadline – to pay an online ransom in return for an unlock code that (in theory) removes the restrictions and restores control or your data.

# BEHAVIOURAL THREATS

As you'll see over the page, it's increasingly tricky for malware to infect your PC with little or no resistance. That's why modern malware is increasingly based on deception, designed to trick you into clicking a web link or opening an infected file. Many of these so-called phishing attempts originate from emails or instant messages. They attempt – with varying degrees of success – to make themselves look genuine, with the aim of getting you to open a file or click a link to visit a fake website where you're asked to enter sensitive security information to 'verify' your details. In actual fact, what you enter is captured by the hacker. There is also a growth in emails claiming to have hacked the user's computer. They claim to have recorded – using your PC's webcam – evidence of you enjoying pornographic websites and aim to make themselves more plausible by inserting an old password stolen from website breaches that's associated with your email account. Most of these phishing emails are caught by spam filters, but occasionally a few will sneak through. Do not respond to any of them.
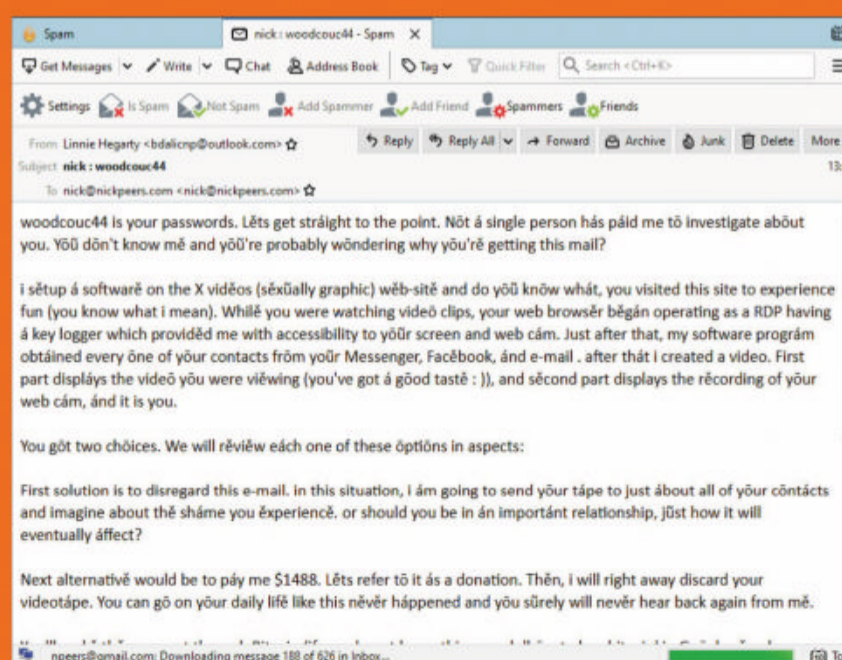


Behavioural threats tend to originate mostly from emails attempting to trick you.

Keep your laptop secure

# Strengthen your PC's security

Audit your current security and find ways to add extra layers of protection. to keep malware at bay.

When it comes to protecting your Windows 10 PC, both antivirus and firewall protection are built into the operating system, and while it's strictly no-frills, Windows Security is capable of keep most malware off your system. We tested it with a range of live malware samples, and it detected them all, throwing up a warning dialog offering to remove or quarantine the malware in question.

Windows itself is also packed with malware-thwarting technology too. User Access Control (UAC) is the confirmation dialog you see whenever you open a file or program that wants administrative access to your system. Windows 10 also introduced the SmartScreen filter, which automatically pops up a warning about program files that aren't digitally signed. Many are legitimate, but it provides you with an extra step of protection. The filter will go even further if it detects known malware, with the dialogue box turning red instead of blue and the warning made crystal clear.

Most malware originates from the internet, which is why your web browser has a role to play too. All modern browsers – including Microsoft Edge – will screen any file after it's been
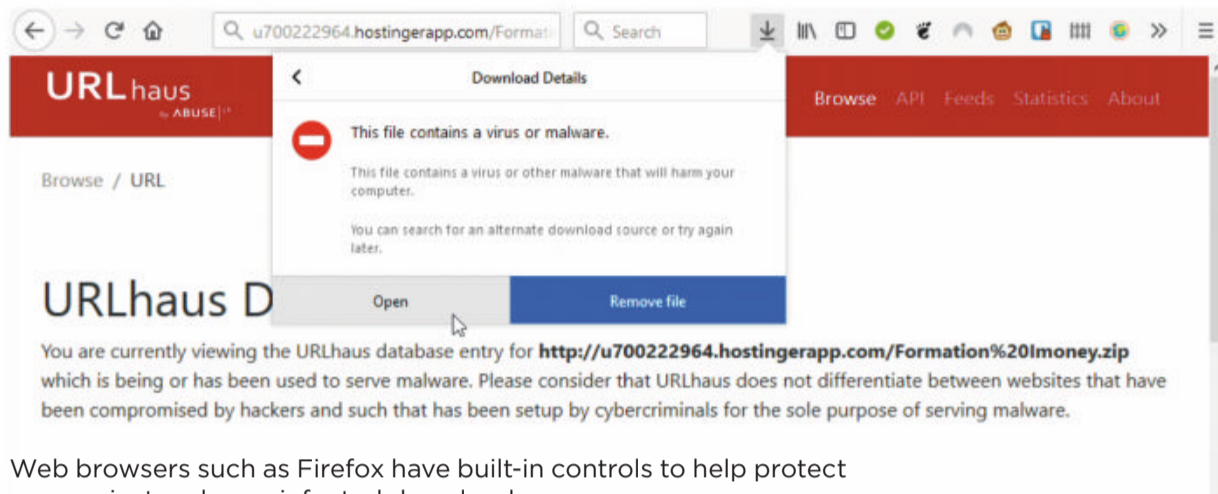


Web browsers such as Firefox have built-in controls to help protect you against malware-infected downloads.

downloaded for potential malware, alerting you if it's known malware. Some browsers, such as Firefox, will even flag a file that's not been downloaded or opened by many people – this should ring alarm bells if you're downloading well-known software from a less reputable website. It suggests the file may have been tampered with, so cancel the download and source it from a safe location, such as the program's own web pages or a trusted mirror.

Browsers also attempt to keep you away from dangerous websites like those involved in phishing scams too – a highly visible warning screen will appear. You can bypass this, but don't say you haven't been warned if you decide to ignore its assessment.

## Third-party protection
If you're looking to add extra layers of protection to your PC, there are numerous free and paid-for third-party packages out there. If you're in the market for third-party protection or want to review your current package as its subscription comes up for renewal, visit **www.av-test.org/en/antivirus/**
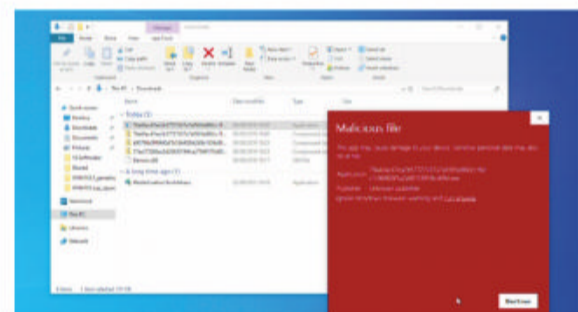


Windows SmartScreen usually throws up a blue dialog for unknown apps, and red for viruses.

# CONFIGURE YOUR FIREWALL

While Windows Security performs well against malware, there's one weak link – its firewall. The Windows Firewall is configured only to monitor incoming connections – in other words, those made to your PC over your network or the internet. It assumes all traffic originating from your PC is legitimate – but this can include any malware that's sneaked through your defences and has established a backdoor connection to the internet. These can then dial home to begin wreaking whatever havoc they've been designed to inflict. This step-by-step guide reveals how to add two-way protection to Windows Firewall using a free add-on package from Malwarebytes, but if you want a more user-friendly alternative then reputable Internet Security packages from the likes of Norton, Kaspersky and Bitdefender all ship with two-way firewalls. A no-cost option is Comodo Internet Security Free. Its firewall works in a similar way to WFC while offering additional functionality such as being able to run your web browser inside a 'sandbox' (isolated container) to protect the rest of your system. See **www.comodo.com/ home/internet-security/free-internet-security.php** for details.
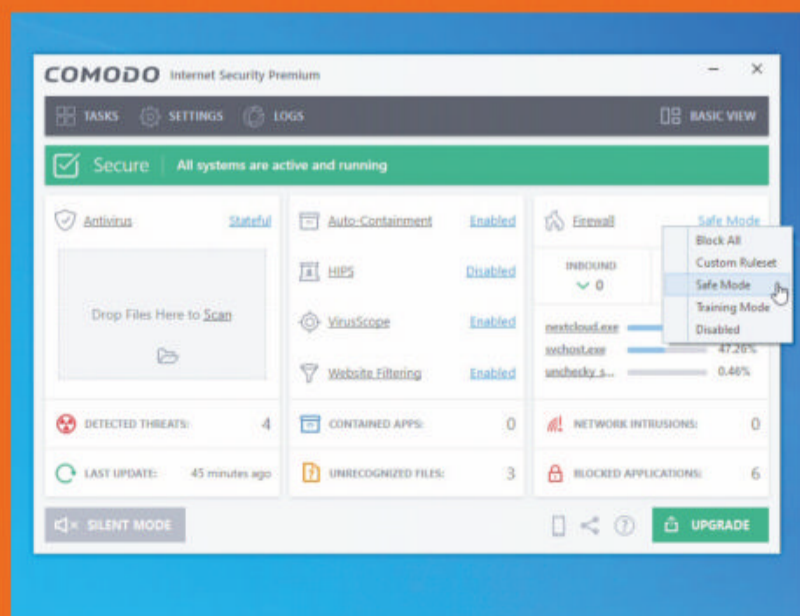


Comodo's firewall runs in 'Safe mode' by default – it'll allow trusted apps to access the internet, only alerting you to unknown ones.

**home–windows/** for a comprehensive list of tests, updated regularly. What you'll notice, though, is that Windows Security now rates highly in malware detection and cleaning tests.

Does this mean there's no need for additional protection? Windows Security provides a good last line of defence, but third–party tools tend to offer a wider range of preventative measures – and if you're still running Windows 7 or 8.1, then switching to a different security package is essential. You should also look to strengthen – if not replace – the built-in Windows Firewall. See below for why, and how.

## Add extra layers

In addition to a firewall, third–party tools provide additional components to help close more gaps in your protection. They'll often proactively scan USB drives when plugged into your PC, and some offer protection for smart devices like webcams too, ensuring they can't be switched on surreptitiously by hackers for spying purposes. Parental controls allow you to protect younger members from more threats than the basic options provided in Windows itself.

Take Bitdefender for example: it comes with an online threat prevention module, which works proactively in the background to protect you when browsing the web or using your network. Built-in anti-ransomware protection is augmented by its Safe Files component,
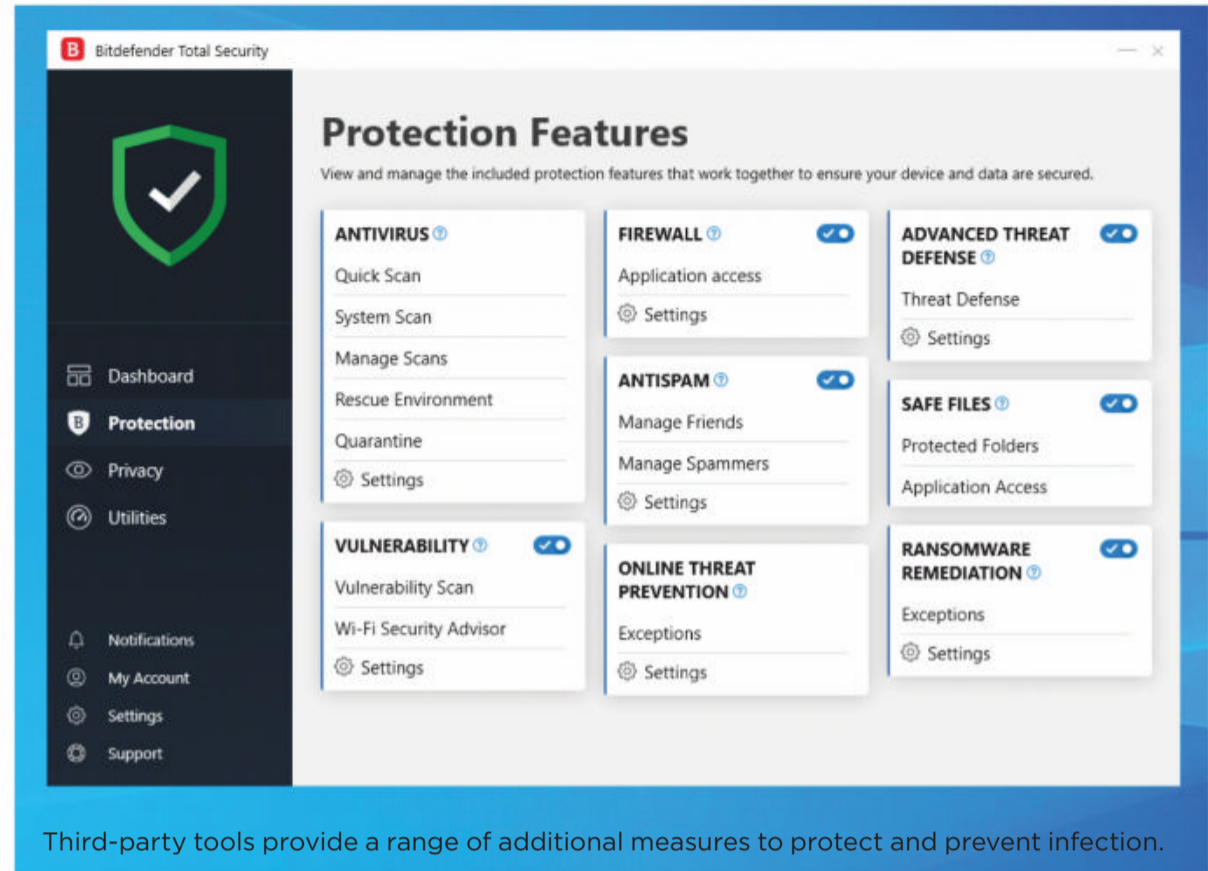


Third-party tools provide a range of additional measures to protect and prevent infection.

which allows you to specify protected folders such as Documents and so on. When enabled, applications can't access these folders without you explicitly granting them permission, serving as an extra block against ransomware.

Many security tools also provide tools that scan for security vulnerabilities – not just in Windows, but your applications and Wi-Fi network too. They'll alert you to weak passwords, outdated programs and missing Windows security fixes.

Whether or not you opt for third–party protection, we strongly recommend you install a secondary, non-conflicting

package to provide another layer of security. Our go-to package remains Malwarebytes Anti-Malware – its detection rates have suffered of late as a primary package, but as backup protection it remains second-to-none. Download the free version from **www.malwarebytes.com** – there's a 14-day free trial offering proactive, real-time protection against malicious websites, PUPs and other threats not covered by some security packages, then revert to a scan-and-remove tool if you don't want to pay the yearly asking price.

# UPGRADE THE WINDOWS FIREWALL
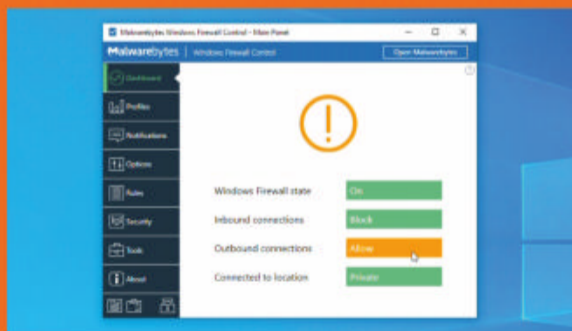


**1** INITIAL STEPS Download and install Windows Firewall Control from **www.binisoft.org/wfc** – once installed, type 'wfc' into the Search box to launch Malwbaytes Windows Firewall Control. The original status screen will reveal it's currently set to Windows Firewall defaults, allowing all outbound connections.
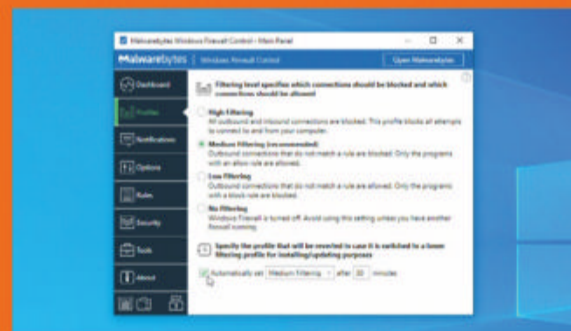


**2** SWITCH THE PROFILE SETTINGS To start monitoring outbound connections, switch to the Profiles section and select 'Medium filtering (recommended)'. Also tick the failsafe 'Automatically set' box. Now switch to Notifications and select 'Learning mode' to switch monitoring on.



**3** REVIEW AND ALLOW All digitally signed and trusted apps will be given network access automatically, but you'll start to see pop-up notifications for other apps. If they're trusted (not all safe apps are signed), click 'Allow this program'. If you're not sure, press 'Block for now and ask me later.

# Remove malware from your PC

Discover what to do when malware strikes – find out how to remove it, plus clean up afterward.

When your security protection works as it should, you'll either enjoy a hassle-free life or see the occasional alert pop up when your antivirus tool spots – and blocks – a potential infection from taking hold. But if your security regimen is compromised, you'll have to take remedial steps to clear any infection from your machine – sudden sluggish performance, random popup alerts and other strange behaviour might all point to infection.

The simplest thing to do is try and run a scan with your existing security tools having first attempted to install the latest updates – if they detect the threat, let them attempt to clean or quarantine it, then reboot and run full scans again. If infections keep cropping up, or you're unable to open your security tool, you may need to attempt to boot into Safe mode to run your security software from where the malware can't cripple it.

## Scanning from Safe mode

There are two ways to enter Safe mode – one method is described opposite in the step-by-step guide. If that takes you back to the normal desktop, try pressing Win + R, typing msconfig and pressing Enter. Switch to the Boot tab, tick 'Safe
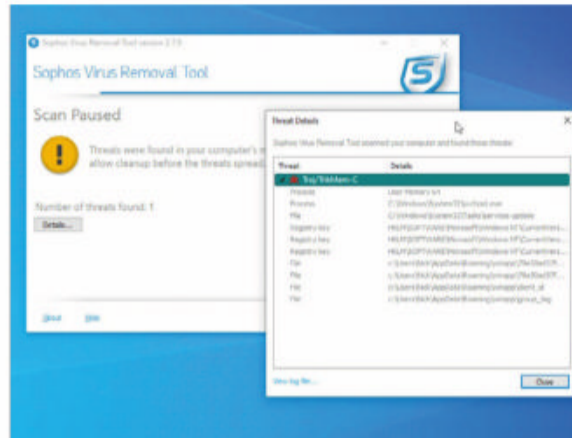


Most anti-virus vendors provide standalone removal tools – try a selection if you're struggling.



Kaspersky's rescue disc – like others – loads a virtual desktop to run its own removal tools.

boot' and select Network before clicking OK and rebooting when prompted.

Some malware removes the Registry keys required to successfully boot into Safe mode – if you're unable to get Safe mode to work following the steps in the guide opposite, skip to the next section. For those who can get into Safe mode, you'll need to enter your user password (any PINs aren't accessible from here) to log in. At the desktop, open your existing security packages, let them update and run full scans.

Hopefully they'll find and remove the infection, in which case reboot back into normal mode (if you used msconfig to get into Safe mode, you'll need to open it again and untick 'Safe boot' before

clicking OK and rebooting) and run final scans to verify the infection has gone.

If you want to be doubly sure the infection has been removed – or your security software doesn't find anything, try enlisting the help of several additional tools. Most security vendors offer free scan-and-removal tools, so Google 'virus removal tools' to see what's available. One example worth trying – because it employs the services of two separate anti-virus engines – is Emsisoft Emergency Kit (EEK), which you can download and run from **www.emsisoft.com/en/software/eek/** for second and third opinions. Also try VIPRE Rescue (**www.vipreantivirus.com/vipre-rescue-virus-removal-tool.aspx**) if EEK doesn't work.

## Use bootable rescue discs

If you're locked out of Safe mode and have access to another, clean PC, visit your antivirus vendor's website on there to track down a bootable emergency rescue disc. If it doesn't offer one, download the Kaspersky Rescue Disc ISO from **https://support.kaspersky.com/viruses/rescuedisk** to a clean PC. Either right-click the ISO and choose 'Burn image' to burn it to CD or DVD, or use a tool like Rufus (**https://rufus.akeo.ie/**) to create a bootable USB drive.

After booting, a separate desktop environment is loaded and the Kaspersky Rescue Tool will automatically start. Let it scan – multiple times if prompted – to ensure all traces of the infection are removed.
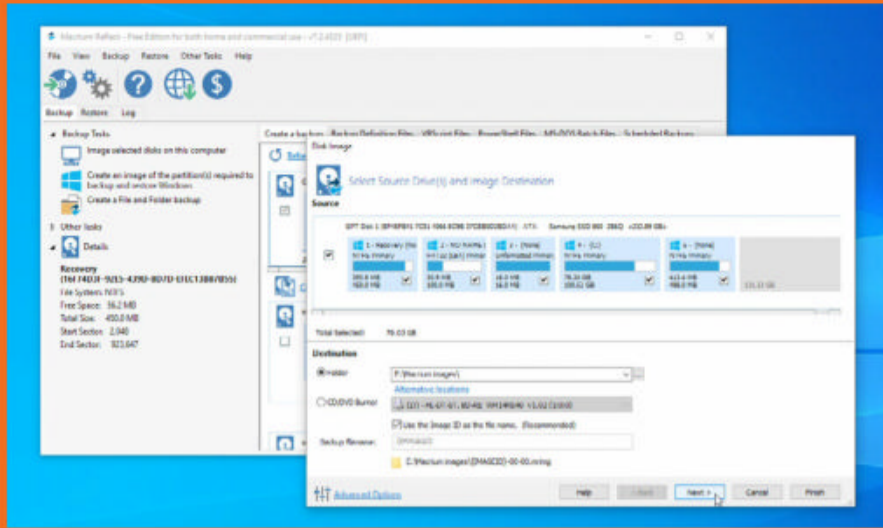


# BEAT BROWSER HIJACKS

If your browser's home page has been changed, or unwanted toolbars and popups appear, you're the victim of a browser hijack. Try Malwarebytes' AdwCleaner from **www.malwarebytes.com/adwcleaner** (scroll down to the green 'Free Download' button). Close all browsers and launch the tool, granting it admin access when prompted, then click Scan Now. Finally, review its findings and quarantine anything you don't like the look of.

# HOW TO Clean up after a malware infection



**1** TAKE A FAIL-SAFE BACKUP Repairing Windows can lead to unforeseen consequences. Start by creating a full drive image using your back-up tool – Macrium Reflect Free (**www.macrium.com**) is our go-to tool. Make sure you've also created emergency rescue media – just in case.
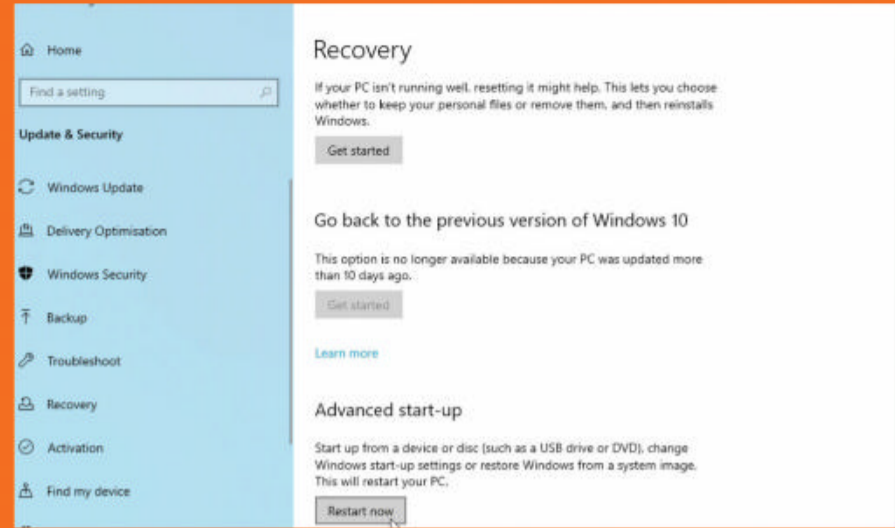


**2** REBOOT INTO SAFE MODE Click Start > Settings > Update & Security > Recovery and click 'Restart now' under 'Advanced start-up'. Choose Troubleshoot > Advanced options > Start-up Settings to select Safe mode (we recommend the 'Safe Mode with Networking' option to retain internet access).
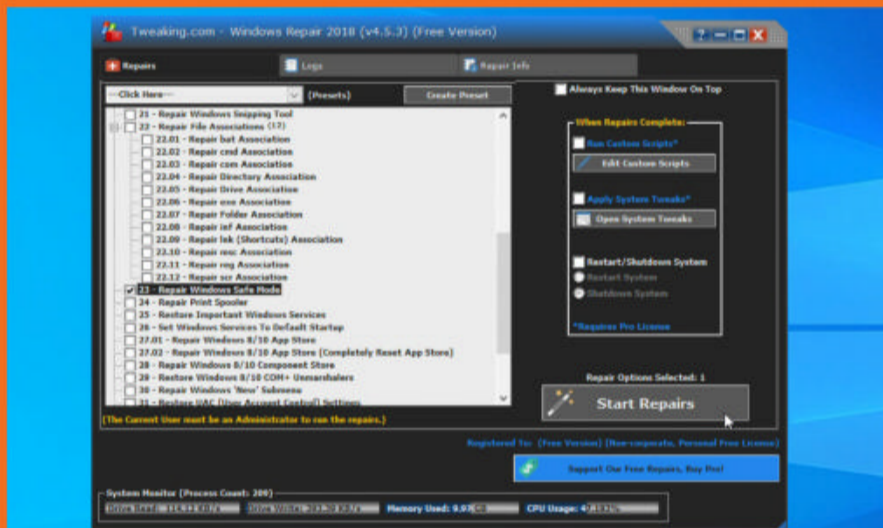


**3** FIX SAFE MODE If Safe mode won't work, reboot or restore your backup if your PC no longer boots. Install and run Windows Repair (**www.tweaking.com**), switch to the 'Repairs – Main' tab, click 'Open Repairs'. Untick 'All Repairs', then choose '23 – Repair Windows Safe Mode' and click Start Repairs. Try Safe mode again.
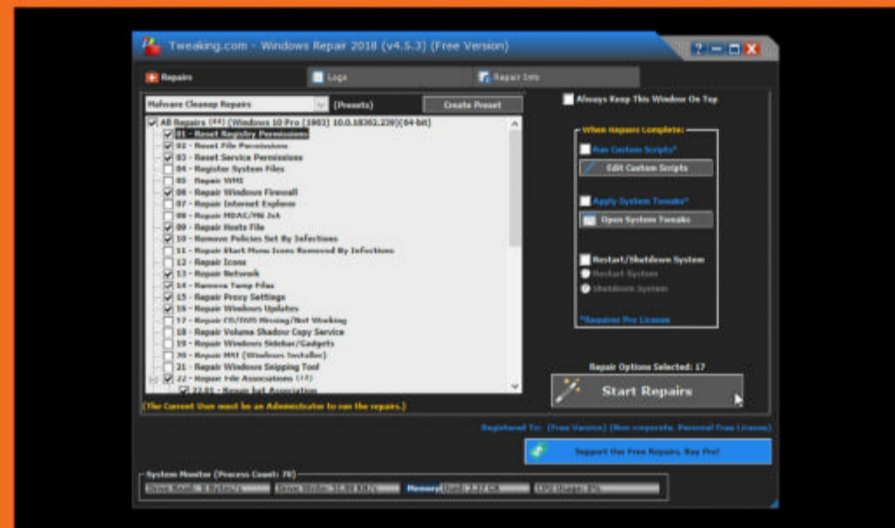


**4** REPAIR FROM SAFE MODE If not already installed, download and run the portable version of Windows Repair. Choose 'Preset: Malware Cleanup Repairs' from the 'Repairs – Main' tab to select repairs linked to malware infections. Click 'Start Repairs' to hopefully fix the worst of the damage. Reboot into normal mode.
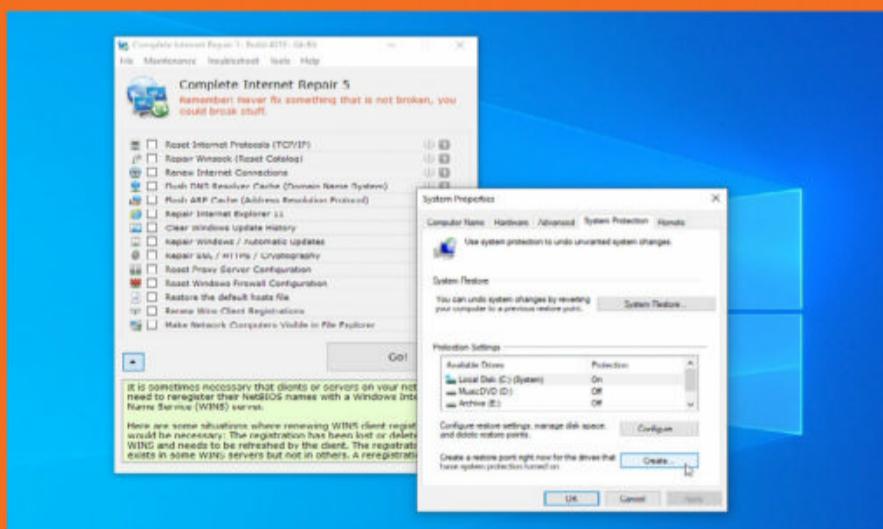


**5** FIX INTERNET PROBLEMS If you're unable to access the internet or network after cleaning up after malware try the repairs offered in one or both of Complete Internet Repair 5 (**www.rizonesoft.com/downloads/complete-internet-repair/**) and NetAdapter Repair All In One (**https://sourceforge.net/projects/netadapter/**).



**6** DECRYPT RANSOMWARE If files have been left encrypted and you have no backups to call on, make a note of the ransomware type from your security logs and visit **www.nomoreransom.org** – upload two of your encrypted files and paste in the ransom note to detect its type and hopefully locate a free decryption tool.

# Expand your protection

Fill in the gaps in your security and privacy with this essential collection of tips, techniques and tools.

You've got the essentials sorted – anti-malware software in place, plus any tools you've downloaded from the previous spread on cleaning malware infections (even if your PC is currently behaving itself, now is a good time to collect them together somewhere safe, like on a USB flash drive). Now you've locked down your PC, what other steps can you take to secure other parts of your online life?

### Secure online accounts

Browse to **www.haveibeenpwned.com** where you're almost certain to discover your trusted passwords of old have been involved in at least one security breach – even if you weren't personally affected, common passwords like 'fred1234' are bound to have been used by others and subsequently exposed too. We recommend installing a strong password manager like BitWarden (**www.bitwarden.com**) to store and generate new lengthy, randomly generated passwords comprising letters, numbers and special characters. All you need to remember going forward is one master password – make sure that password is both memorable and long, not easily guessed
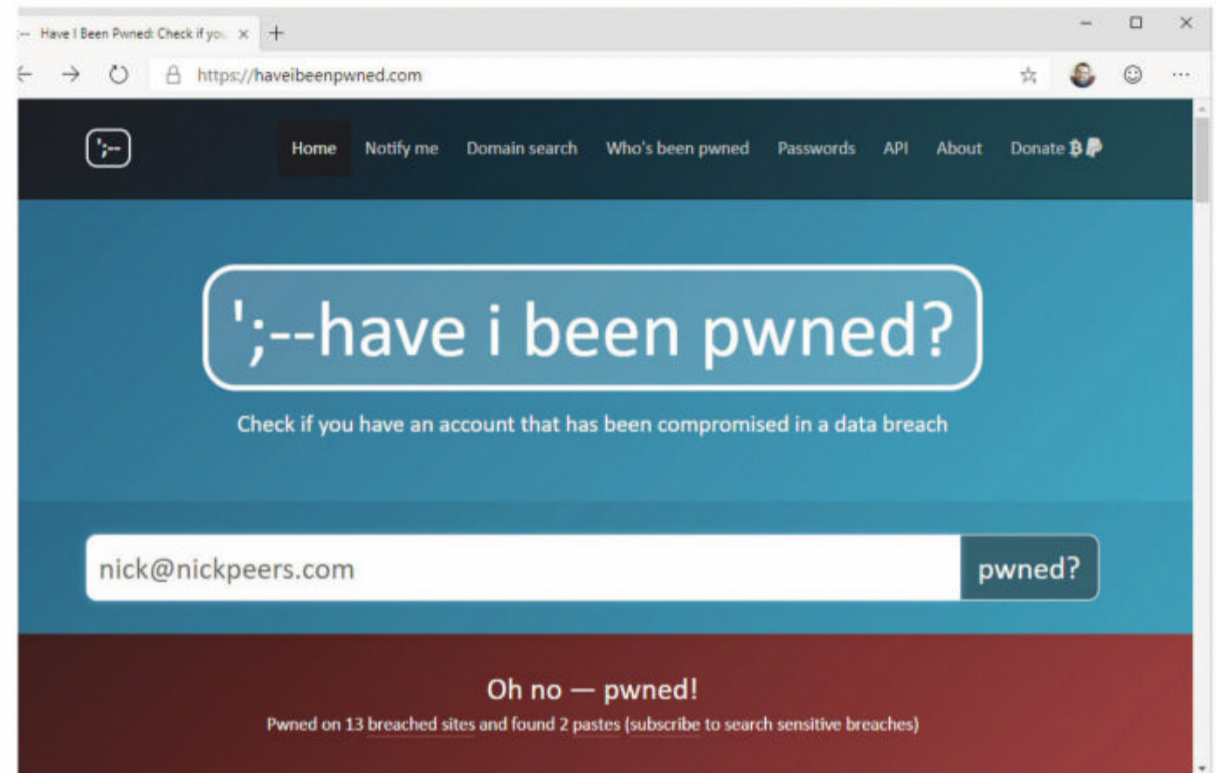


Don't panic if you find your email address appears in various site breaches – just make sure your passwords have been changed.

and a mix of letters and numbers.

Add an extra layer of protection to your BitWarden password vault – and other key online accounts – by adding two-factor authentication (2FA) to your login. This prevents anyone from getting into your account without physical access to your phone – even if your password is compromised. 2FA codes can be delivered by email, mobile text or to an authenticator app – email isn't secure (see below), while text messages require you to have a mobile signal when sent. The best option is the authenticator app – we currently recommend Authy (**https://authy.com/**), which can be installed on more than one device (including your PC) and codes accessed even when offline.

## FILL IN THE GAPS

Windows Security has plenty of built-in protection against system exploits, rootkits and the like, but there are still gaps – many behavioural related – that you can close with the help of free software. Start by keeping an eye on programs that need software patches with the help of Patch My PC (**https://patchmypc.com/home-updater-overview**). Add protection against PUPs with Unchecky (www.unchecky.com), while IObit Uninstaller (**www.iobit.com/en/advanceduninstaller.php**) has a Bundleware section that can help root out PUPs already on your system. Worried about the security of sensitive data backed up to the cloud? Ensure your files are protected by an extra layer of encryption before being uploaded with Cryptomator (**https://cryptomator.org/**). Add extra protection against potentially harmful websites by adding traffic-light security ratings to web pages and search engine results using one of Norton's Safe Web (Chrome, Firefox and Edge) or BitDefender Traffic Light (Chrome and Firefox). Search your browser's add-on store for the appropriate plugin. Finally, want to screen email before downloading it? Install PopTrayU (**http://poptrayu.sourceforge.net/**) or POP Peeper (**www.esumsoft.com**) to preview all of your accounts from one convenient app.
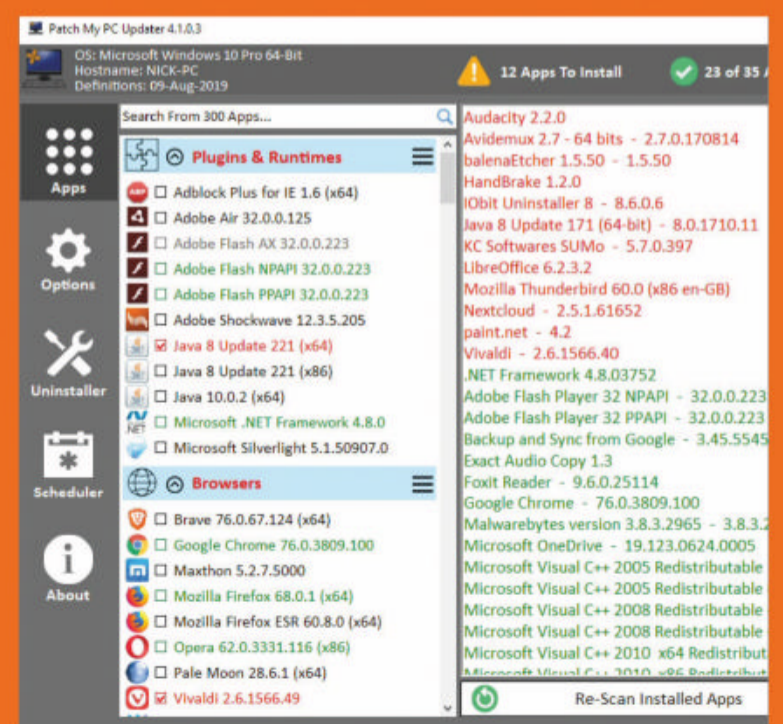
## Secure internet access

Virtual Private Networks (VPNs) serve two major purposes: one, they encrypt your internet traffic on insecure networks such as public Wi-Fi hotspots, but they also mask that traffic from your Internet service provider too. By connecting to a VPN server in a different country you're also able to trick internet services as to your actual location, enabling you to bypass many geographic restrictions – for example, enabling you to access catch-up TV while abroad on holiday. WindScribe (**https://windscribe.com**) offers a generous 10GB free bandwidth a month with support for servers from 10 countries including the UK, US and Switzerland. A Pro package comes with tools for blocking ads and trackers as well as malware (US$9.00 a month or US$49 for a year).

While VPNs encrypt your data in transit, they don't hide it from the services you're connecting to, so you'll need to continue to take steps to protect your web browser. Make use of private or incognito windows when browsing – which allegedly don't store any tracking information after they've been closed. We say allegedly – it's still possible for your traffic to be monitored by your internet service provider.

One way to tighten this security is by enabling so-called DNS over HTTPS if your browser allows you to do – for example, Firefox users should open Options > General tab, then scroll all the way down and click Settings under 'Network Settings' before ticking 'Enable DNS over HTTPS' (with the default Cloudflare provider) before clicking OK. This prevents man-in-the-middle attacks and eavesdropping on the websites you visit.

Also look to install add-ons to help block trackers and malicious advertising. The step-by-step below reveals how to use Disconnect to monitor and block invisible trackers – after installing it, install AdBlock Plus (**https://adblockplus.org/**) for a sensible approach to blocking intrusive and potentially dangerous adverts without removing all adverts.

Email is notoriously insecure – unencrypted and easy to intercept. Traditional encryption techniques involving PGP only work with contacts who apply it to their own email. One workaround is to sign up for a free ProtonMail account (**www.protonmail. com**). Mail between ProtonMail users is automatically encrypted, while you can configure sensitive messages so non-ProtonMail users are directed to a secure, encrypted web link to read – and reply – to the message.

Protecting yourself when chatting with others and using social media is a must too. Install the Facebook Container add-on for Firefox, for example, and you can isolate Facebook from the rest of your web activity by forcing it to run in a sandbox – that way it can't spy on you through tracking cookies. Similarly consider switching from well-known, but not necessarily secure, technologies such as Skype and WhatsApp to Signal (**https://signal. org**), an open-source chat tool that works on your phone and PC desktop and offers secure end-to-end encryption.
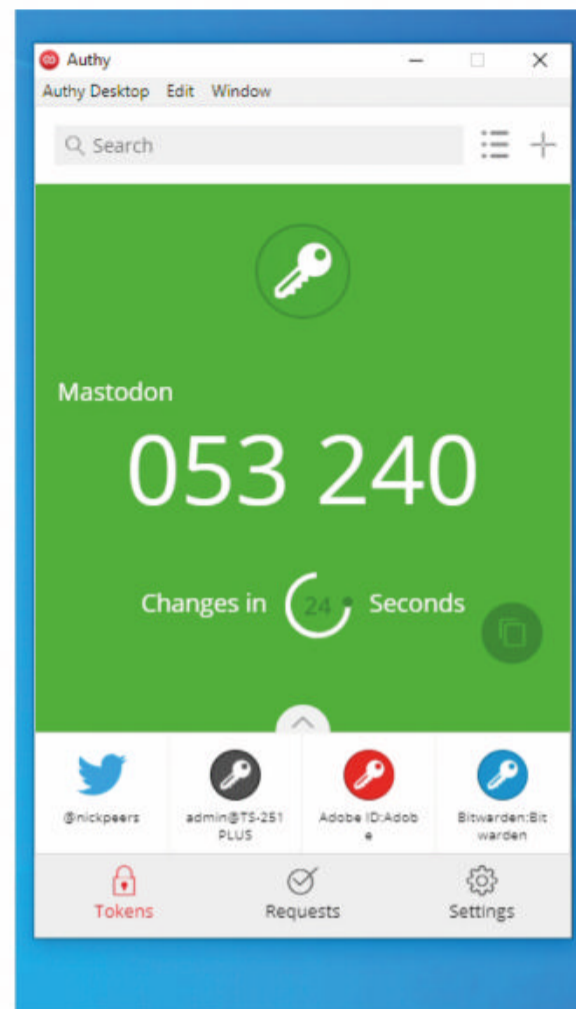
No more excuses – protect your online accounts by implementing 2FA now.

# TRACK THE TRACKERS
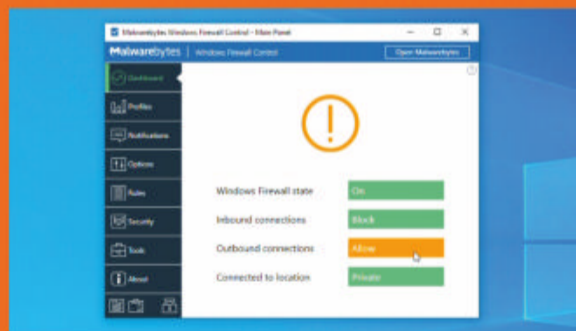
**1** INSTALL DISCONNECT Go to **https://disconnect.me/disconnect** and click 'Get Disconnect' to locate the plugin in your browser's add-on store, then install it from there. Once installed, you'll see the Disconnect button appear in your browser toolbar. You do not need to donate if you don't want to.
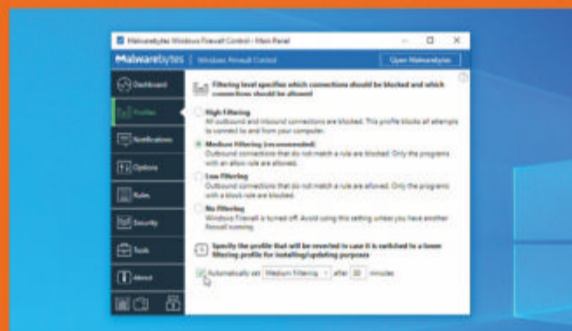
**2** MONITOR WEBSITE Now browse to one of your favourite websites. You'll see the Disconnect button display a number – this is the number of trackers it has detected. Click the Disconnect button for a summary, split into four sections – click one to reveal the specific requests made.

**3** BLOCK TRACKERS Any trackers ticked and marked green are blocked by default; grey trackers are safer, but can also be blocked by ticking the box. You'll see statistics revealing how much time is saved not processing the trackers. Click the 'Visualize page' button to see where the trackers go.

# PERFECT PASSWORD PRIMER

Human laziness, complacency, general failings, and unending ingenuity to subvert systems have undermined passwords forever. It's time to next-gen your security, and save all your passwords!
By Neil Mohr

In any system, humans will find a way to subvert the rules for their own gain. It's a recurring theme: from skipping class, cheating in games, fixing the banking system, and exploiting welfare, down to stealing from work, and gambling in Las Vegas. So it shouldn't be a surprise that most humans choose the lazy option when it comes to password security.

It's too easy just to say humans are lazy, and pin terrible password security on that. Humans will always attempt to game systems at both ends, which is why passwords are being hacked and people want to avoid memorising them in the first place. It's not good enough to just use a strong password; we now live in a world where so much is tied up with our online lives that hackers are doing more and more to break into online accounts.

So, we're going to look at the whole subject of password security, and hence online account security, how we can choose better passwords, how we can make our lives easier but also safer, how we can increase protection beyond passwords, and how hackers attack and use your account details.

Some of this advice you'll have probably heard before, some of it is hopefully new, but by the end, you'll be terrified enough that you'll overcome your human propensity for laziness, and get up off your bottom, and protect your passwords!

Let's start by scaring the heck out of you. There has been a host of research on password security, made much easier by the huge number of database breaches in recent years. One of the widest-ranging research efforts was by Google, published mid-2017 in its *Data breaches, phishing, or malware? Understanding the risks of stolen credentials* paper (**https://research.google.com/pubs/pub46437.html**).

Some sweet nuggets from that little cache include the fact that the researchers swept over 1.9 billion non-unique account usernames and password credentials. These were taken from a variety of leak sources, but mostly blackhat security forums. An insane 76 percent of these could be (or already were) easily converted to plain text (best practice is to hash and salt stored credentials). The researchers were able to reverse an impressive 36 percent of hashed passwords, using a suitable keyword attack.

Of those stolen via phishing attacks, 49 percent were from Americans. When it came to pure security leaks, 39 percent of credentials were linked to Americans. As for credentials stolen via keyloggers, Brazil accounted for the highest amount in this group at 18 percent.

Credential leaks appear to happen regularly these days. The largest ever remains the initially hushed-up Yahoo leak, back in 2013, in which pretty much every Yahoo account ever was leaked,



Google Chrome can manage and synchronise passwords across your devices.



A well-integrated mobile app handles online accounts and local app logins.
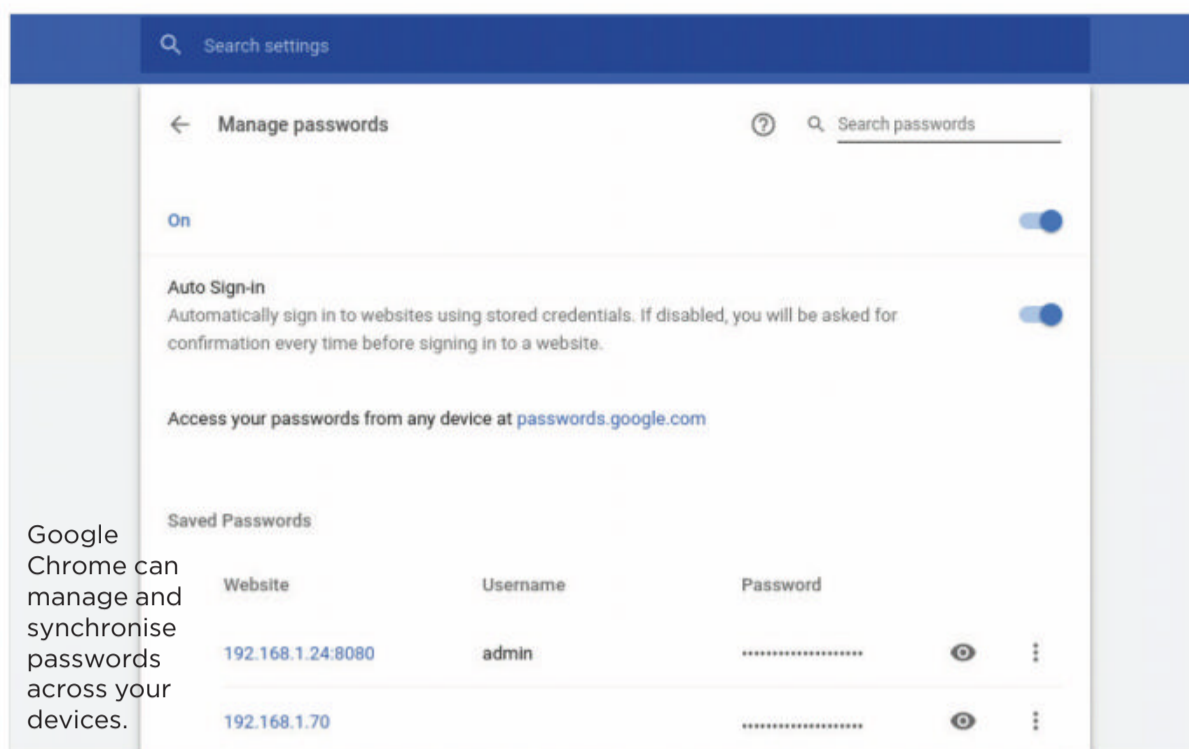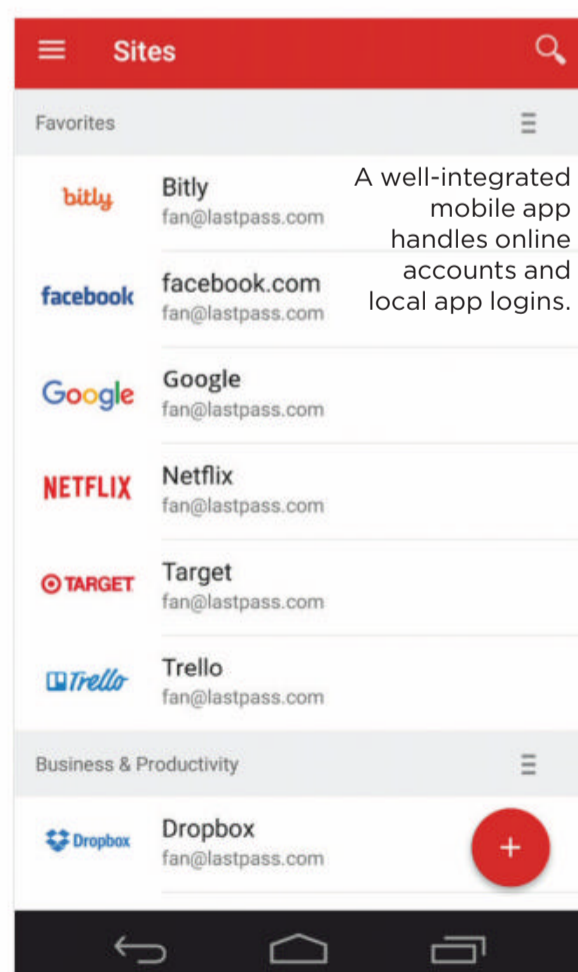
totaling three billion. Adult Friend Finder topped 412 million, the 2017 Equifax breach hit 143 million users, while MySpace, Adobe, LinkedIn, Dropbox, LastFM, NexusMods, and more have all had their leaks, each individually releasing millions of users' details.

These leaks show the basic issue with password reuse: If you are using the same password across all of your online accounts, it just takes a single leak to contain that password, and all your accounts are compromised.

## Science save us!

So the logical next question is: What makes a secure password? Entropy. That means the level of randomness in a system. By randomness, we mean true randomness. It's not enough to have a long password, it has to be long and truly random. We stumbled across a lovely analysis of poor password creation by WPEngine, at **https://wpengine.com/unmasked**.

Among many things, it shows that password creation is a truly gender neutral pursuit – men and women can live equally in a world with terrible passwords. It's worth a read – as well as being funny and interesting, it highlights a lot of general failings us humans have when it comes to creating passwords.

The obvious beginnings are the standard bad passwords: '123456', and any variation thereof, 'password', 'qwerty', and again any variation of those. Obvious stuff. Another issue is that many password guidelines are bad – forcing upper-case letters, for instance, because people tend to just

capitalise the first letter; forcing at least one number, because people just put '1' at the end; or demanding a password of at least a certain length, because people use a pattern on the keyboard. For example, the seemingly random 'ADGJMPTW' is actually people typing 2–9 on a smartphone number pad. This is what happens; it doesn't make for strong passwords, because they're easier to guess with a much lower entropy.

It's that human nature thing. One group wants to protect a system, another wants an easy life, so it circumvents the rules, a third group is attempting to break in. So, how do we make stronger passwords?

A few years ago, a Dropbox engineer, Dan Wheeler, wrote a blog post (**https://blogs.dropbox.com/tech/2012/04/zxcvbn-realistic-password-strength-estimation**) referencing Randall Munroe's classic *XKCD* 'correcthorsebatterystaple' cartoon (**https://xkcd.com/936**) on password entropy, alongside Mark Burnett's earlier research (**https://xato.net/perilous-password-policies-3ad038aa33b1**). Dan's post is long and complex, and focuses on what makes a strong (high entropy) password, alongside how that can be easily measured and communicated to the user. Conversely, Randall's point was part password strength, but he was largely extolling the need to make password systems human-friendly.

We don't get into the nitty-gritty too much, but effectively a good password is a long password. Simple. The *XKCD* approach is to use a memorable series of words or phrase, usually painting an odd scene, such as the classic example of a 'correct horse battery staple', but it could

Perfect password primer
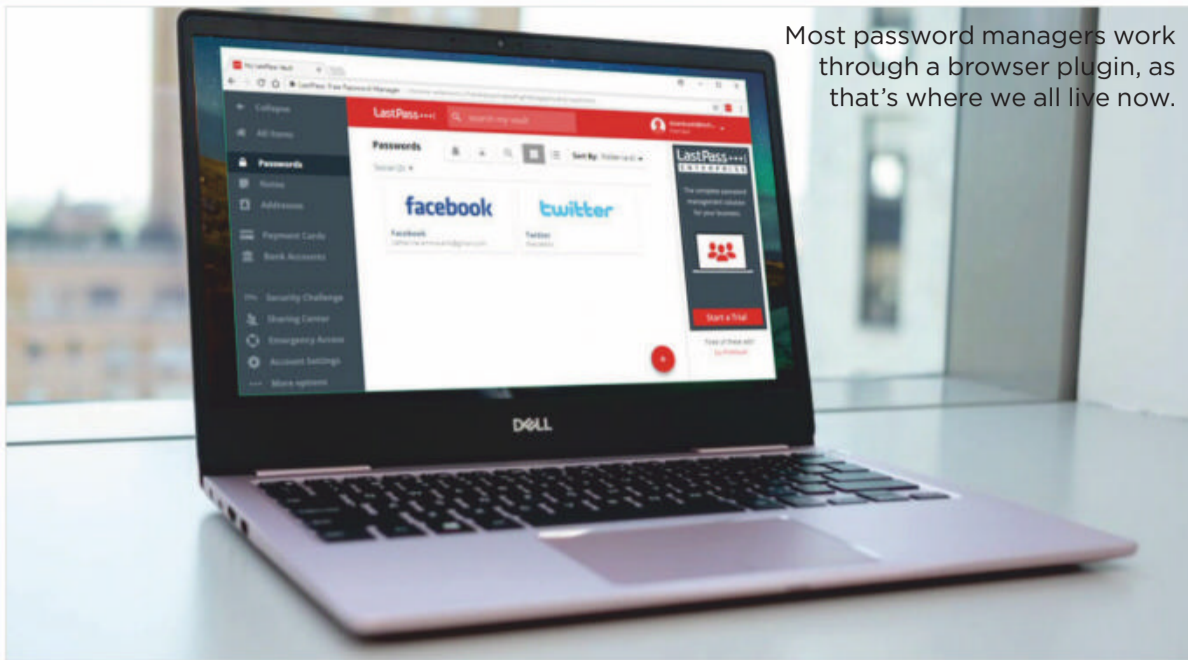


Most password managers work through a browser plugin, as that's where we all live now.

be a phrase such as 'basketball on a unicycle flying high'. From a memorable point of view, this taps into techniques used by memory experts. Of course, throw in some numerals and symbols, and it's even stronger.

None of this addresses the core issue, though, that we now have a seemingly endless number of online services to use and try, each with their own password and login. Even making passwords memorable wouldn't solve the innate issue of having to remember them all. The solution to that is a password manager.

## Microsoft save us!

The obvious place to start is to ask what tools Microsoft provides in Windows 10 or beyond. The blasé answer is none. Windows doesn't come with any specific password management tool. What Microsoft has done is build a basic

password manager into its Edge web browser, which enables those saved passwords to be synchronised across your Windows accounts, and to any other instances of Edge you might be running – Edge on Android, for example. But what if you're not on your Windows account? What if you're not on Windows at work or home? What if you're using Chrome or Firefox? What if you want to create a strong password? What if a site is demanding non-standard credentials? The Edge password manager is basic at best, and fails to help in all but the most simple of scenarios.

## Browsers save us!

How about a browser that you might actually want to use? The most widely used web browser at the moment is

Google Chrome, and it comes with a reasonable password manager built in. To kick off, if you've logged in with your Google account, it syncs passwords across all of your devices and operating systems (Windows, macOS, Linux and Chrome OS), and is, of course, available on Android and iOS devices, too. Google also offers an online service at **http:// passwords.google.com** that enables you to log in and access passwords from within any web browser on any device.

Beyond passwords, Google Chrome also supports intelligent form filling. You can enter a default address, phone number, and email address, and if Chrome thinks you're filling those details in, it offers to try to auto-fill entire forms or individual elements. Alongside this it has a secure credit card storage option, if you find the idea of Google having your credit card details a good one... What could possibly go wrong?

Chrome's basic but smart enough password manager means that as long as you're logged in to your Google account, a right-click in a password field offers the option to generate a secure password. There are no options, it just provides a random password of suitable length. It then, of course, saves and manages that login and password for you. You can set exceptions and manage the saved passwords from within the Advanced Settings. Access to these is protected via a system prompt that ask you to enter your regular Windows password.

# ALTERNATIVE MANAGERS



We're going to suggest three other commercial password managers – the ones that crop up most often, and generally offer similar features at similar costs. So, it's down to you which you feel works the best. The first is 1Password.com; prices start at US$2.99 per month for a single user, and US$4.99 for a family account for four people.

DashLane (**www.dashlane.com**) is a major player and offers a number of plans that will suit a wide range of consumer and

business uses. The basic plan is free for all, but is limited to working on a single device. The paid home plan is US$3.33 a month, and supports unlimited devices, password sharing, and Yubikey 2FA support. A business plan starts at US$4 per user.

Our final option is **Keepersecurity.com**. It has a similar structure to DashLane, but opts to have yearly subscription pricing. The basic single-user package is US$29.99, effectively US$2.50 per month, and offers unlimited devices with sync,

unlimited password storage, secure cloud backup, fingerprint access, and web access with support. A family option costs US$59.99 for five users.

There are, of course, a host more password managers. You can find a vaguely independent list on Wikipedia at **https://en.wikipedia.org/wiki/List_of_ password_managers**, or our sister website *TechRadar* maintains a list of free(ish) password managers at **www.techradar. com/1325845**.

The other main browser worth a mention is Mozilla Firefox, although it doesn't provide much more functionality than Microsoft Edge. It synchronises your password across its own Firefox account to any supported OS or devices. It doesn't support forms, and won't generate passwords for you, but it does offer an independent master password to protect access.

## LastPass save us!

So, browsers generally leave us wanting more when it comes to real password management. You could get by with Google Chrome, but we can do better. Enter the world of dedicated password managers. We're going to concentrate on LastPass (**www.lastpass.com/**) in this main section – for alternatives, see the various boxes throughout the feature. It's certainly one of the prime options to look at when it comes picking a password manager; the free account provides the majority of the functions people require, while the paid-for premium edition is just US$2 per month.

LastPass is a multi-device, multi-OS, multi-browser tool. It largely works as a browser plug-in for the big five: Chrome, Firefox, Safari, Edge/Internet Explorer, and Opera. It runs on all the main desktop OSes: Windows, macOS, Linux, and OpenBSD. And for mobile devices, there's Android, iOS, and Windows Phone support. Plus, you can log in to your LastPass password vault



One-time use access codes enable emergency access if you lose your 2FA device.
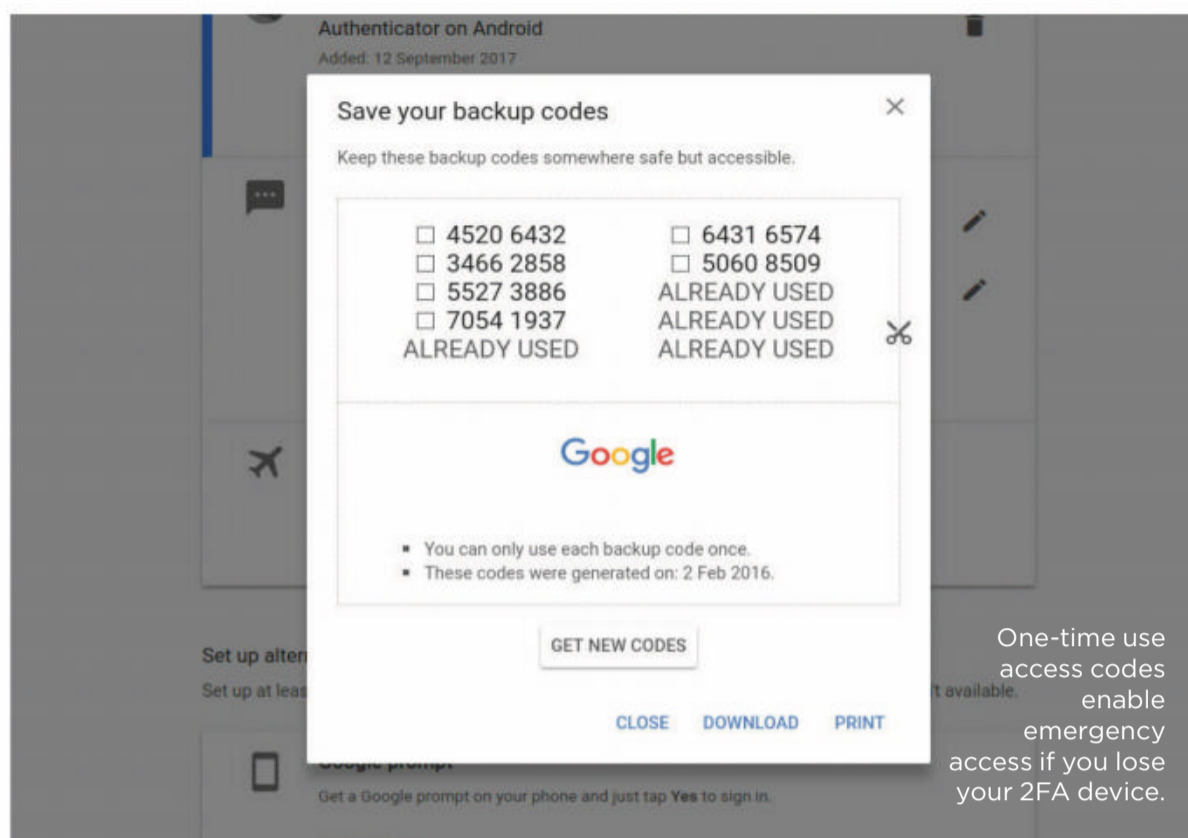
through any browser, too.

The name LastPass comes from the fact that your LastPass account password will be the last password you need to remember; it'll take care of all the rest. So, what does it do? The main use is via a browser plug-in and apps on your mobile devices. As you create new accounts or log in to existing ones, LastPass stores your usernames and passwords, or offers to generate new passwords as accounts are created.

The LastPass password generator is pretty sweet. You can choose any length, up to 100 characters, select any mix of upper and lower-case, choose the quantity of numbers to use, and decide

whether or not it should use symbols. There are also advanced options for avoiding ambiguous symbols or attempting to make your new password pronounceable.

Accounts can be grouped into categories and searched. You can add notes and opt for automatic logins, to help speed you into accounts. LastPass also supports automatic filling of standard forms: names, addresses, emails, phone numbers, bank accounts, credit cards, and custom fields. There's a general encrypted notes tool, too. It also offers a warning for insecure forms, plus a security audit of existing accounts that you might import from your web browser. Two-factor authentication is

# THE OPEN-SOURCE WAY

We like open source; it might not always produce the most polished-looking software – [cough] GIMP [cough] – but for security software, its publicly scrutinisable code tends to provide peace of mind, while largely ensuring a project can continue even if the original organisation or developer packs up their bags, as the source code stays open to be picked up by someone else.

We're going to highlight two strong open-source candidates. The first is the well-known KeePass.info. Don't confuse this with the largely defunct KeePassX. org that hasn't been updated for two years. There is a fork called KeePassXC.

org, which is up to date, but we'll stick with KeePass as it has many unofficial respins for Android and other devices that make it easier to use.

KeePass isn't as straightforward to use as the commercial alternatives; the main hoop you need to jump through is for multi-device synchronisation, where a third-party cloud service, such as Dropbox or Google Drive, needs to be roped in. But the breadth of support, custom options, and feature set is unmatched, with no fees to pay.

The other strong open-source option is Bitwarden (**https://bitwarden.com**). It offers an excellent free model, a US$1-a-



month family subscription that supports up to five users, a basic business version at US$5 per month, plus enterprise options. It's a modern, slick, open-source application supporting Windows, Linux, macOS, all the major browsers – including Opera, Tor, and Brave – plus Android and iOS devices. If you're a fan of open source, we suggest you give it a look.
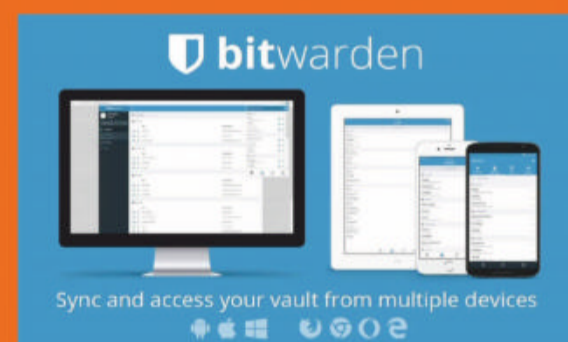
Perfect password primer



Online gaming service Steam has offered secondary authentication for many years.
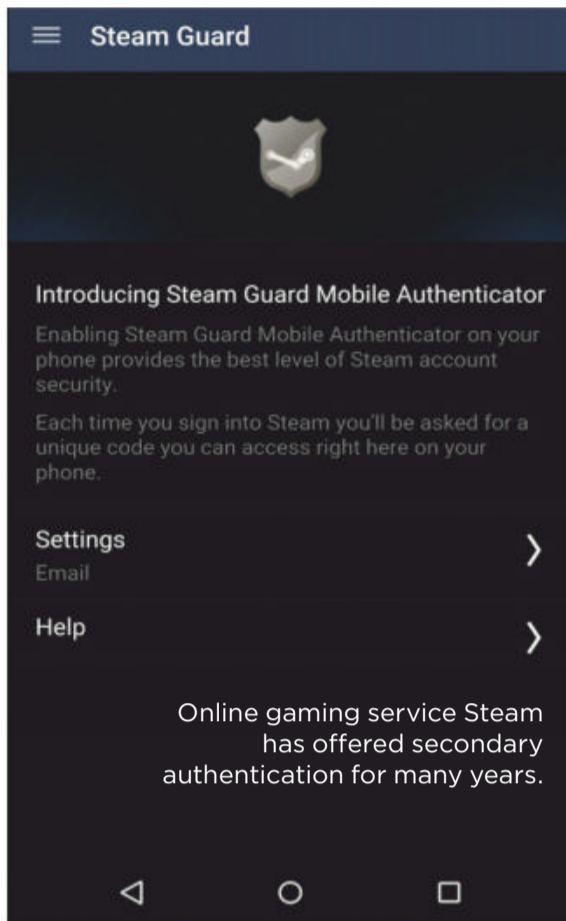
supported, too – we cover this later. The paid-for service expands password filling to other applications, on both Windows and Android – LastPass can fill in a program's password and fields; handy these days as more programs require some type of login for subscriptions.

Once installed, it's worth looking at LastPass's Preferences. At Windows Help & Advice we like to add a log-out time, so if you leave your PC alone, it logs itself out after an hour, for example.

LastPass isn't the only password manager to offer all these features, but it does provide an idea of the expanded capabilities, improved security, and genuine ease of use a dedicated service offers.

But with great power, comes great responsibility. A service such as LastPass requires you to use a strong master password; if that is hacked, someone will gain access to every service you use. Or if you forget the password, LastPass can't restore your master password, as it is never sent it in the first place, as a deliberate security measure. It might sound like we're putting all our eggs in one basket, but what do you want – an individual basket for every egg, or just one awesomely secure basket?

Even security-conscious businesses can be hacked and run into issues (**https://en.wikipedia.org/wiki/LastPass#Security_issues**). LastPass has had a number of vulnerabilities exposed, and even had a successful hack attack on its own servers in 2016. But as a security conscious company should, LastPass offers bug bounties – which it honours – and is open about breaches with its users, while using best practice on its secure storage.

So even the server breach in 2016 meant users' own passwords remained secure.

## Gaben save us!
A question that security experts started to ask a while ago was: Is there anything better than passwords? You won't like the answer, but it's unlikely we'll ever be completely free from passwords, although two-factor authentication offers a respite. Called 2FA or TFA for short, the premise is that people require two forms of identification, AKA authentication; typically, the first is a strong password (something you know), and the second can be your fingerprint, your delightful face, or a generated one-time-use passcode (something you have).

As you might have spotted, many phones are now using fingerprints and face scans to authenticate access. Financial institutions are even happy enough that NFC-equipped phones can authenticate credit card transactions. Some systems (LastPass, VeraCrypt) accept USB flash drives and specialist USB keys (Yubikey, **www.yubico.com**) as a second form of authentication.

Steam is a good example of a service or organisation that was quick to provide two-factor authentication. You should be familiar with its email verification, which sends a code to your default email address, while more recently, Valve introduced the Steam Authenticator app for smartphones and tablets, which is required if you're messing around with its trades.

# AUTHENTICATE WITH GOOGLE



We're going to highlight the Google Authenticator as a prime two-factor authentication (2FA) tool. Install it on your phone, then fire up the service you want to protect with 2FA. LastPass uses Google Authenticator (among others) to do so. Using that as an example, head to LastPass Vault > Account Settings > 'Multifactor options'. Click the Edit button and Enable it. Use the Barcode option to display a QR code. On your phone, open Google Authenticator, tap '+' and click 'Scan barcode', then point your phone at the on-screen QR code. You should now find that LastPass has been added to Google Authenticator.

Anytime someone tries to access your LastPass Vault from a new device, they must enter the current code (this updates every 30 seconds) before access is granted. There's an option to allow access for 30 days, before another 2FA prompt appears on that device. Without your phone, there's no access.

2FA is great, but does have a couple of caveats. Firstly, the service using it mustn't be monumentally stupid. It was discovered that some services could have 2FA circumvented by simply calling up and providing some basic personal information, making the use of 2FA more security theatre than actual security. The second is that potentially the 2FA code is locked to the one phone. Technically, a rooted Android device enables you to transfer the Google Authenticator secrets, but if you get a new phone, ensure you disable 2FA on your services, before wiping your old one. Otherwise, you could be locked out of vital services. LastPass keeps the QR code secret, so you can have it on multiple devices, and transfer it later on – provided that you can log in, of course.

Because of the magical nature of cryptography maths, many services also offer offline access options, usually via a bank of single-use passcodes that you can print or scribble down, and keep safe somewhere. This means that if your phone is lost, stolen or broken, you will still be able to access your accounts.
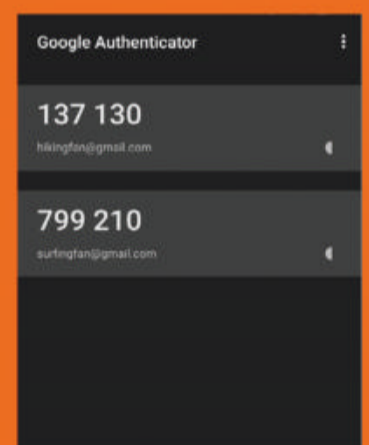
# PROTECT YOUR DATA

Encrypt files, folders, and even entire drives to keep your information secure.

Worried about the security and visibility of your data? Do you have sensitive files you want to keep away from potentially prying eyes? Worried that your cloud backup isn't as secure as it might be? Concerned that the data on your laptop might be vulnerable to theft? Want to dispose of files – or an entire PC – without compromising the data (including previously deleted files) on it? You've come to the right place.

In this feature, we explore numerous options for protecting your data, both data stored on your PC and that backed up elsewhere, whether on local storage or in the cloud. We also reveal how to ensure all data you delete is shredded beyond recovery, too, enabling you to pass on a PC

or drive to a new home without having to worry about the data previously stored on it.

When it comes to sensitive files, the solution lies in a process called encryption. File encryption works using cryptography to scramble the contents of files so they're unreadable without the correct authentication – usually a password that is used to unlock an encryption key, which in turn decrypts the file so it's readable. Some encryption can be further strengthened by the requirement of additional forms of authentication such as so-called key files or physical devices, like smart cards.

Encryption keys are created using special algorithms. Common examples include Advanced

Encryption Standard (AES) and Twofish. The higher the bitrate, the more secure the key, so 256-bit is better than 128-bit, and 512-bit is better than 256-bit. Encryption is a resource-heavy process, particularly as bitrates increase, so be prepared to see protected files take longer to open or save. If you have a modern CPU, you'll find AES is by far the quickest encryption standard, thanks to the implementation of hardware-accelerated AES encryption on supported processors.

Encryption can be performed on individual files or entire drives, and that's where we begin our feature, with a comprehensive guide to scrambling the files on your PC. Turn the page to get started.

When it comes to encrypting individual files or entire drives, there are numerous options available. If you're running the Pro, Enterprise, or Education version of Windows 10, you'll find built-in options exist in the form of BitLocker and EFS – the box opposite reveals how BitLocker works and what you need to run it. EFS – Encrypting File System – enables you to individually encrypt files or folders using your Windows password as the encryption key. If the drive is stolen, the files are unreadable without your Windows account password.

To encrypt one or more files or folders, select them in File Explorer, right-click the selection, and choose Properties. Click Advanced, then tick the box next to Encrypt contents to secure data. Click OK then Apply – you're prompted to encrypt the parent folder if applicable for greater security. Make your choice, then click OK. EFS is a simple but relatively weak way to encrypt files. If you're looking for something stronger, or don't trust Microsoft with keeping your data secure, read on.

## Simple, fast file encryption

If you only need to encrypt individual files on a semi-regular basis – or wish to encrypt files before sharing them with others – the open-source tool AES Crypt (**www.aescrypt.com**) is all you need. Download and install the program, then going forward, simply right-click the file you wish to protect, and choose AES Encrypt. Enter a strong password – the more characters, the stronger the encryption – and click OK. An encrypted copy of the file with an .aes file extension is created, unreadable to anyone who doesn't know the password.

If you want to share the file with others, send them the encrypted version, then communicate the password
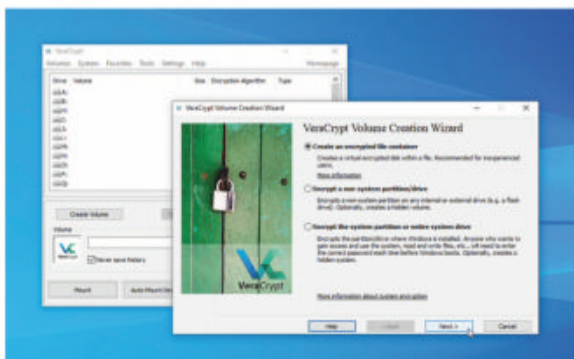


VeraCrypt's wizard makes it easy to create any kind of encrypted drive.
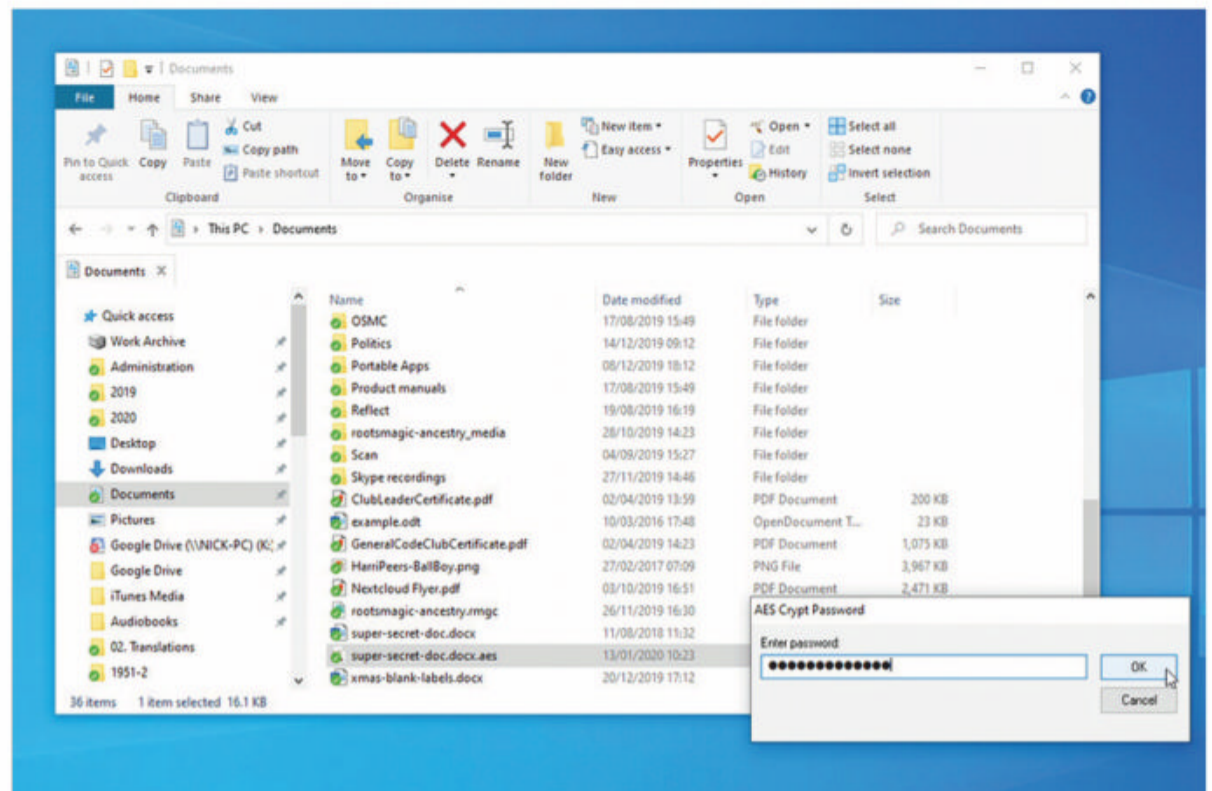


AES Crypt won't delete your original file after creating an encrypted copy.

separately and securely. They need to install AES Crypt before double-clicking the file and entering the password required to extract the decrypted original.

It's also possible to encrypt Office documents – but encryption is only effective in Word 2007 or later when first AES 128-bit, and more recently (from Office 2016) AES 256-bit, encryption is employed. To do so in Office 2007 or later, select the File tab and choose Info > Protect Document > Encrypt with Password.

If you want stronger encryption for individual files or folders, Gpg4win (**www.gpg4win.org**) works in a similar fashion to AES Crypt, with the added bonus of allowing you to encrypt files using public keys protected by passphrases for additional security. After installation, launch the Kleopatra tool and choose File > New Key Pair, then select Create a personal OpenPGP key pair to get started. Once done, you can then encrypt files by right-clicking them in File Explorer and choosing Sign and encrypt to use your key (you can also encrypt files with a simple password, too, if you prefer).

## A one-stop solution

AES Crypt and Gpg4win are perfect for occasional encryption, but you'll need to re-encrypt your files each time you make changes to them. If you want a more comprehensive, flexible solution, VeraCrypt (**www.veracrypt.fr/en/**) pretty much does it all. It can be used in a variety of ways to meet most people's needs – like BitLocker, you can encrypt

entire drives, including your Windows boot drive, but you can also restrict its use to a specific set of sensitive files using a smaller virtual encrypted container, which resides as a file on your hard drive.

The app is available for Windows, Mac, and Linux, so you can use it across all your computers. There's a portable version available, too, which can do everything except encrypt your boot drive. After downloading and installing (or extracting to your portable apps folder), launch the program – Veracrypt-x64.exe if you're running the portable version – and you will find yourself at the main VeraCrypt window.

## Create a virtual drive

The VeraCrypt Volume Creation Wizard now opens, with Create an encrypted file container selected by default. This is the safest option, because it merely creates a single file on an existing hard drive, inside which all your sensitive data will be stored for you. There's no risk to any other files or drives. To proceed, click Next.

Two types of volume can be created – to simply protect the data if the drive it's on is lost or stolen, leave Standard TrueCrypt volume selected, and click Next again. Skip to the next section. You'll also see an option to create a hidden volume, with an explanation about why you might want one. Hidden volumes are created inside standard TrueCrypt volumes, hiding themselves in their free space.

First-time users should select Hidden TrueCrypt volume then Normal mode to create a standard TrueCrypt volume inside which your hidden volume will be created. If you've already created a
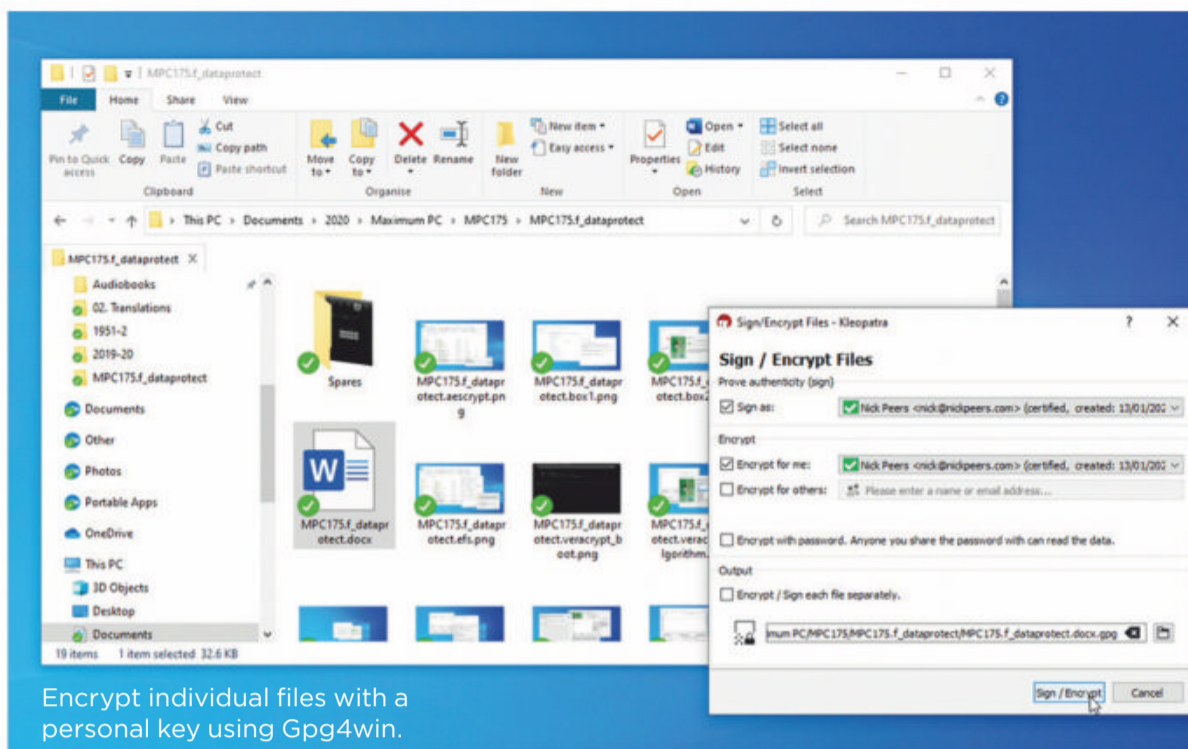
Encrypt individual files with a personal key using Gpg4win.

standard volume, you can choose Direct mode instead when prompted, and follow the prompts to set it up inside your standard TrueCrypt volume. In either event, the wizard follows a similar process to that for standard volumes, as described below.

One tip if you plan to create a hidden volume: Be sure to save selected files to the standard volume. An empty standard volume would arouse suspicion among those you're trying to hide your data from.

## Set up a standard volume

Click the Select File… button, browse to your USB thumb drive, then type a new file name into the File name box. Avoid using a file extension – this can be problematic – and click Save. Click Next to choose your encryption options for the volume. Five encryption algorithms are supported: AES, Serpent, Twofish, Camellia, and Kuznyechik – select one at a time for a description. Beneath these are no fewer than ten combinations of two or more algorithms for those who want multiple layers of encryption. The truly paranoid can click the Test button next to an option to verify VeraCrypt's implementation of the selected algorithm is compliant with certain standards.
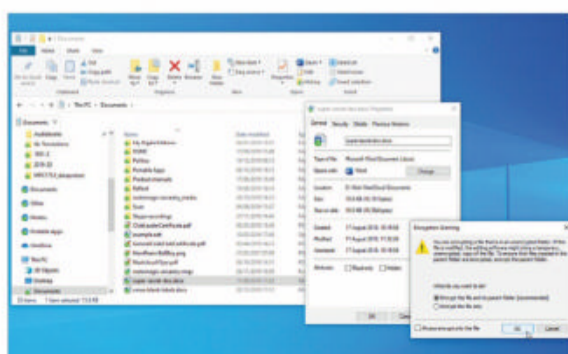

Windows 10 Home users don't get access to native encryption tools.

Click the Benchmark button to open the Algorithms Benchmark window, then click Benchmark to compare the performance of each encryption algorithm. The process of encrypting and decrypting data will have an impact on disk write/read speeds, and you can compare the different algorithms (single and combined) from here. Straight AES encryption is recommended for most people, or AES combined with Twofish if you want a second layer.

Beneath the encryption algorithm, you'll see a section on hash algorithms, complete with a handy link explaining how they work. These are basically used to generate the encryption keys and salt (random data used to protect your password from hackers). Five hash algorithms are currently supported, but for most people, the default SHA-512 is fine – you might choose SHA-256 if performance is more important than security.

## Extra authentication

Once you've chosen your options, click Next. You're now prompted to set a size for your file container. Choose a figure based on how much data you need to encrypt and how much free space is available. Click Next to enter a password – you'll need this to access your files in future, so make sure it's memorable (or stored somewhere secure, like a self-hosted Bitwarden password manager), but also tough to crack. Try to make it at least 20 characters in length.

Gain additional protection by ticking Use keyfiles and clicking the Keyfiles button. This adds another layer of protection: Not only do you have to enter your password correctly, but you also need to select whichever file (or files)
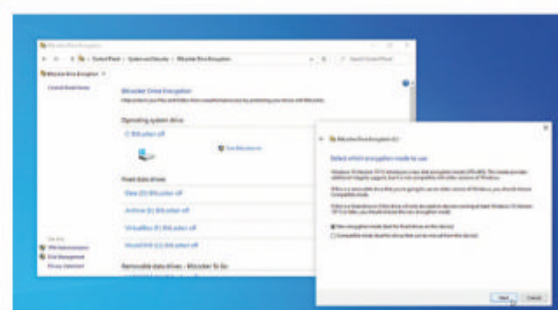
## BITLOCKER DRIVE ENCRYPTION

If you're using a higher-end version of Windows – Professional, Education, or Enterprise – and you're looking to encrypt an entire drive, you might like to use the built-in BitLocker tool. It can be used to encrypt fixed and removable drives, as well as your Windows boot drive, making it possible to protect the contents of your laptop should it be stolen.

Type "bitlocker" into the Search box and click Manage BitLocker. You'll see a list of all available drives in the main window. Expand one and click Turn BitLocker on. If you're looking to encrypt the main system drive, you may see an error about your PC not having a compatible Trusted Protection Module. Check your motherboard specifications – you may be lucky and simply need to enable TPM support in the BIOS (look in the Security section).

You're prompted to create a backup of the recovery key required, then follow the wizard, selecting appropriate choices depending on your drive and PC setup. Run the recommended BitLocker system check, and you should be able to use your drive while it's being encrypted.

Fixed or removable data drives are protected by password or a compatible smart card – TPM module not required. When you plug in the drive or reboot Windows, you need to provide the password or plug in the smart card to unlock the drive.

BitLocker is relatively straightforward to use, but relies on your trusting Microsoft, because unlike the open-source VeraCrypt, its code isn't available for audit. You're also restricted to its 128-bit or 256-bit AES encryption.
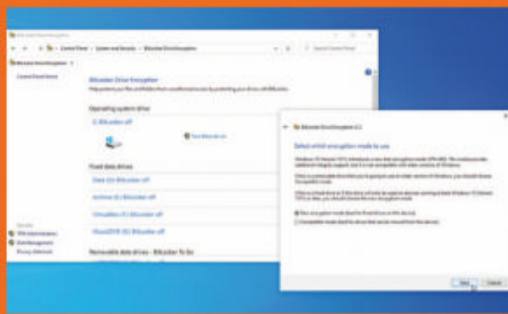
## ENCRYPT IN PLACE

It's possible to encrypt an existing data drive without wiping it in VeraCrypt using Encrypt in place. But there are drawbacks. Unlike encrypting your Windows installation, the drive won't be available while it's being encrypted. Also, when done, you're prompted to assign it a different drive letter – this isn't necessary as we'll explain shortly.

Choose Encrypt in place, click Next, read the warning, and click Yes. You're prompted to set encryption and authentication options, then asked to move your mouse randomly to strengthen the encryption keys, before ending up at the 'Wipe Screen'. This allows you to shred unencrypted files after the drive has been encrypted to prevent them from being recovered by undelete tools later. Only the most paranoid should consider anything other than None (fastest) or 1-pass (random data).

Click Next, then Encrypt. Click Yes (you may need to click Yes again if the drive is in use, to dismount it), then wait for the drive to be encrypted. Once done, read any warnings, and click Finish. To keep the same drive letter, right-click This PC in File Explorer, and choose Manage. Identify your encrypted partition using its drive letter, right-click it, choose Change Drive Letter and Paths, select the current drive letter, and click Remove, then OK. You should now be able to select the drive letter in the main VeraCrypt window, and click Auto-Mount Devices to follow the advice in the main feature to access the drive. If you wish to decrypt the drive permanently, select it, and choose Volumes > Permanently Decrypt.
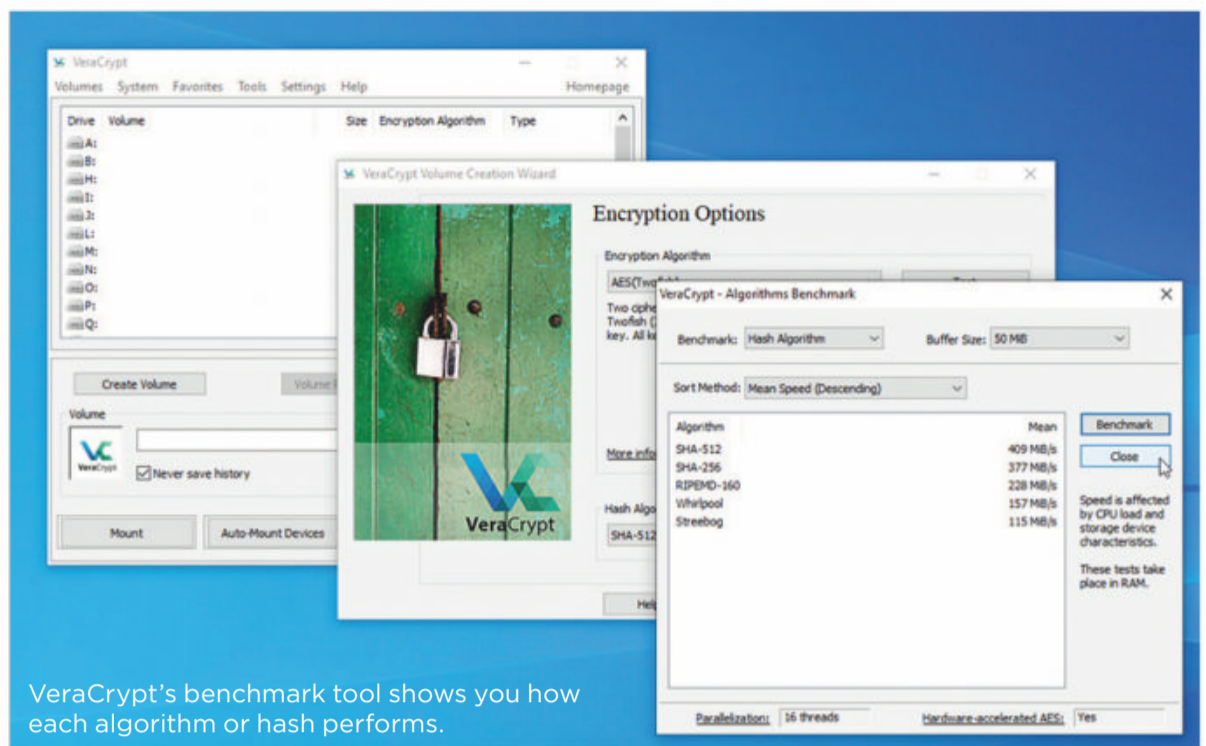


VeraCrypt's benchmark tool shows you how each algorithm or hash performs.

you choose to be linked to your container. These files can be already present on your hard drive – choose a compressed format such as MP3 or Zip – or you can have VeraCrypt generate a new random key file from scratch. Either way, make sure the files are backed up somewhere safe, because if they're deleted or the first 1,024KB of data is changed, your vault will be impossible to access.

Checking the Use PIM box creates an additional step after clicking Next, where you can set a custom Personal Iterations Multiplier. The default setting (485) prioritises security over speed when mounting the volume after each system boot – should you wish to reduce the time taken, you can set a lower value, but make sure you've set a lengthy password.

### Format and mount

After clicking Next, you're asked if you plan to store files larger than 4GB in your new virtual drive – this determines which filesystem is set as the default in the next step (exFAT if yes, FAT if no). Click Next and you're ready to configure and format your volume. You can change the filesystem here – NTFS and ReFS are also available – plus choose whether to perform a quick format (not
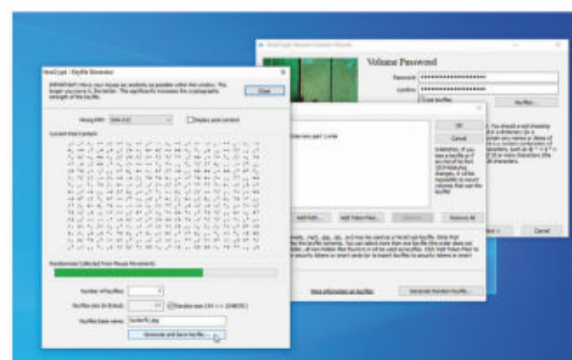


Key files add an additional layer of security to your encrypted data drives.

recommended). Checking Dynamic means the file containing your encrypted volume isn't formatted as its actual size, but instead increases in size as you add content to it – this comes with several warnings, not least of which are severely degraded performance and reduced security.

You'll see a prompt to move your mouse within the VeraCrypt window to improve the cryptographic strength of the volume's encryption keys. When you've configured the drive and the Randomness Collected From Mouse Movements meter is full, click Format, and the encrypted volume is created. Wait until the confirmation dialog box appears, then click OK followed by Exit to return to the main VeraCrypt window, ready to access your encrypted container for the first time.

Select a free drive letter from the list and click the Select File button to choose your encrypted container. Click the Mount button and then enter the volume's password before – if applicable – clicking the Keyfiles… button to select the required files that will give you access to your container when you click OK.

You'll see a Mount Options… button; clicking this reveals options such as opening the volume in read–only fashion, or assigning it a specific drive label in Windows. If your volume contains a further hidden volume, be sure to tick Protect hidden volume against damage caused by writing to outer volume to safeguard its contents.

After clicking OK, wait while the volume is mounted – you should see your encrypted container appear in the main VeraCrypt window. It can now be accessed like any other drive – copy or

save files directly into here to ensure they're protected going forward. When you've finished with the drive, right-click its entry in the VeraCrypt window, and choose Dismount to lock it away from prying eyes.

## Encrypt Windows

VeraCrypt can also be used to encrypt your entire Windows installation. All files remain encrypted on your disk even in use – they're simply decrypted on demand to allow Windows and your apps to run normally without exposing the data to potential problems, such as sudden power loss.

This form of encryption is particularly suitable for those who carry sensitive information with them – typically on a laptop. Take a drive image backup before you begin, then launch VeraCrypt and choose Create Volume > Encrypt the system partition or entire system drive. Again, standard and hidden options are available (click More information if you like the idea of hiding your OS from view – it's a long, detailed subject, and involves creating a 'decoy' OS).

Assuming you simply want to encrypt the drive, leave Normal selected and click Next. You can opt to simply encrypt the Windows partition, or the entire drive (so all partitions on the primary hard drive). If in doubt, encrypt the system partition only – you may get a warning when attempting to encrypt the entire drive about losing access if it has a so-called 'inappropriately designed' BIOS.

The next step informs VeraCrypt whether you have a single-boot or multiboot system, and then it's a similar process as for creating an encrypted virtual drive.

There's just one caveat: you can only protect your system drive with a strong password; key files aren't supported. You also need to create rescue media – don't skip this step, because it's required to both permanently decrypt your drive and provide protection against corruption.

Different media is required depending on whether your boot mode is EFI (USB flash drive) or MBR (CD/DVD) – just follow the prompts to create and verify the media. The recovery media is tied to your specific PC and the current password you've assigned to your boot drive. If you make any hardware changes, you need to recreate it.

You next see the Wipe Mode screen,
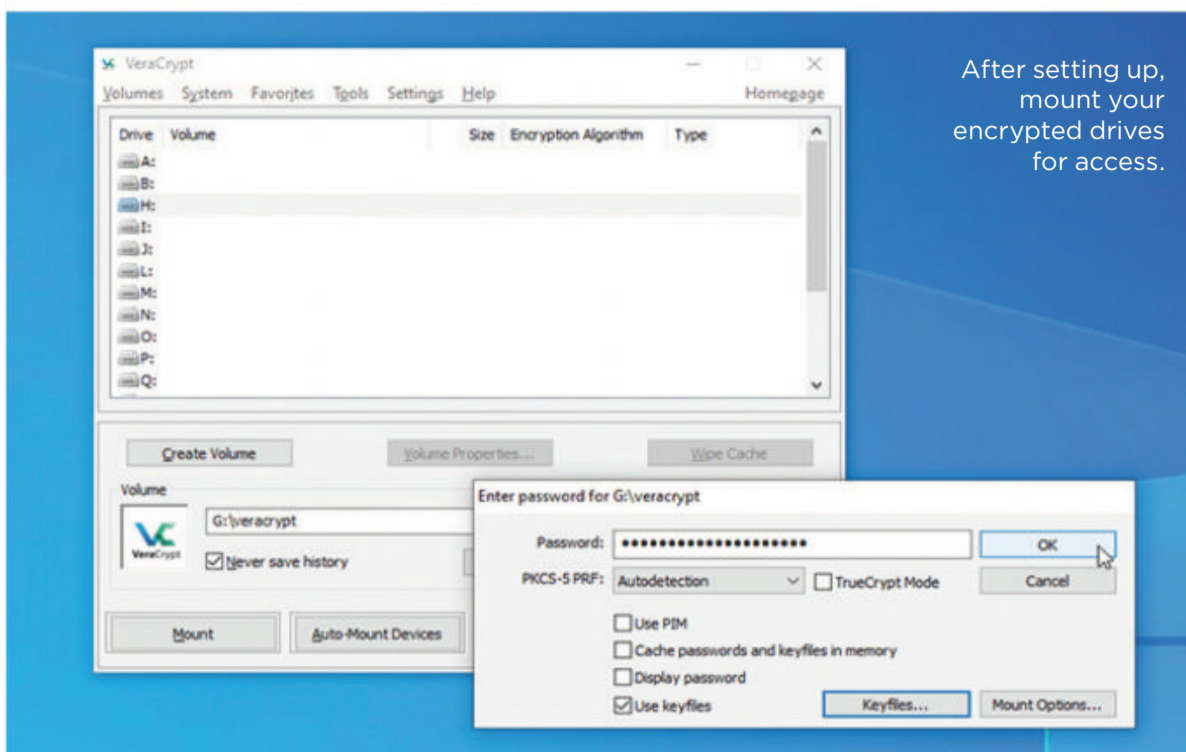


After setting up, mount your encrypted drives for access.

which enables you to securely overwrite the unencrypted copies of your files after they've been encrypted – the more passes, the slower the process, so unless you have reason to be truly paranoid, none or just '1-pass' should be sufficient.

## Test and encrypt

You're now ready for the drive to be encrypted – first, a pretest is run to verify everything works as it should do. Your PC reboots, and you're prompted to enter the password you just set up. When prompted for the PIM, just press Enter unless you manually specified this value. Wait for the password to be verified – then Windows boots as normal.

If the test passes, click the Encrypt button and VeraCrypt starts to encrypt your drive's contents (a Defer button is also present if you wish to back up data first – you're then prompted again the next time Windows is restarted). Unlike with encrypting non-system volumes, you can carry on using your PC while the drive is encrypted. Once

complete, your computer's contents are protected against theft and other threats, ensuring any data stored on the drive is secure.

## Encrypt entire drives

VeraCrypt can also be used to encrypt other drives and partitions, from internal data drives to USB thumb drives. As with all major operations, we strongly recommend you first take a full image of your hard drive before starting the process – just in case. Once the drive is safely encrypted, you can safely delete this backup. However, if you plan to keep the backup, check out the box overleaf about encrypting your backups.

The creation process is similar to setting up virtual drives. Start by selecting Encrypt a non-system partition/drive on the first page of the wizard. Choose whether the volume will be a standard one or hidden, then click Next. Click Select Device... to choose your target drive or partition.
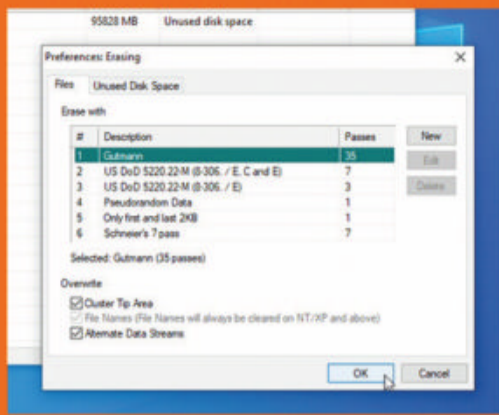
The next step is crucial – you have a choice between Create encrypted volume
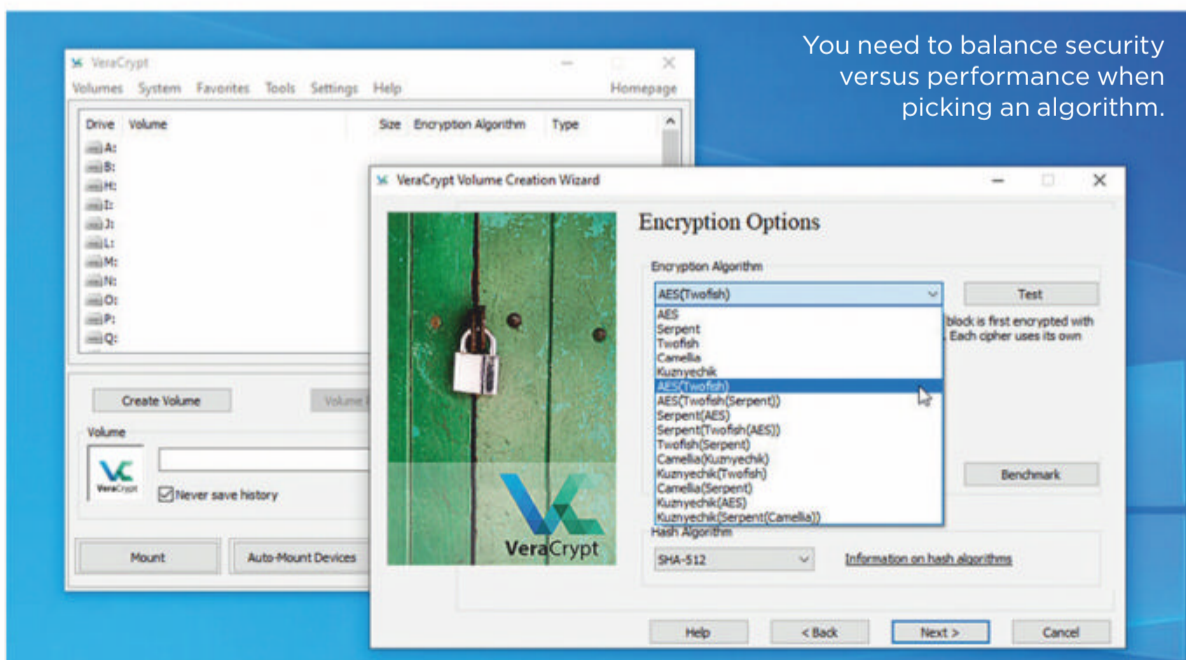


You need to balance security versus performance when picking an algorithm.

65

Protect your data



# SHRED DATA SECURELY

When you delete a file, it's not physically removed from your PC; instead, the first few bytes of the file are overwritten with a tag that tells Windows that the file is deleted and the space it currently resides in is available when writing other files to disk. It speeds things up, but it's not good for security.

Until the file is physically overwritten by another file, its contents are still retrievable. What's more, even if the file is overwritten, it might be possible to retrieve part or all of it using sophisticated file recovery techniques. So, how do you protect yourself against that kind of technology?

Thankfully, there are tools that can securely wipe data from your drive. One that's free and open source is Eraser (grab the latest stable version, 5.8.8, from **https://eraser.heidi.ie/ download**). During installation, enable the Windows Explorer extension to allow you to securely shred any file by right-clicking it and choosing Eraser > Erase. What about files you've previously deleted? Eraser can securely wipe all free space to make deleted files unrecoverable – right-click the drive in File Explorer, and click Erase > Erasing Free Space.

Open the main Eraser program and you can set up on-demand and scheduled tasks to periodically shred specific files, folders, or free space. By default, Eraser wipes data using the Gutmann technique – if this is too slow, choose Edit > Preferences > Erasing to choose a different method, including one of two used by the US Department of Defense.

and format it (destructive, and best for empty drives or drives with no data worth keeping) and Encrypt partition in place. The latter is much slower but preserves existing data . If creating an encrypted volume from scratch, the process is virtually identical to creating virtual drives.

Once the drive has been encrypted, read any warning messages, then click Finish. To mount the drive, select the drive letter you wish to assign to it, then click Auto-mount Devices. Enter the credentials required, wait, and then the drive is mounted and available.

Ordinarily, you have to do this every time you restart Windows – to have the drive automatically mount when you log into Windows, right-click it in the main VeraCrypt window after mounting, and choose Add to Favorites. Be sure to check Mount selected volume upon logon before clicking OK. In the future, you will be prompted to provide the password and any key files each time you log into Windows, and then the drive will be available.

One problem with this approach occurs if you've moved system folders – such as user folders or those linked to cloud services – on to this encrypted storage space. You get errors about missing folders before you unlock the drive. If you've encrypted your Windows boot drive, you can get around this by ensuring the password on your data drive is the same as that required to unlock your Windows boot drive, then choose Add to System Favorites – this way, the drive is unlocked with your boot drive, and available when Windows loads.

## Encrypt cloud backups

VeraCrypt can protect your files locally, but copy them anywhere else, and they're left unprotected. The box opposite reveals what to do about protecting local backups using the same types of algorithms with suitable backup software, but what about those files you back up to the cloud? Cloud providers claim to encrypt your files, but sometimes that only applies to the way the files are transferred – when stored 'at rest' in the cloud, they may be left unencrypted, and therefore potentially vulnerable.

Even where encryption is provided, is it true end-to-end encryption, where only you possess the all-important encryption keys required to decrypt the files? Some cloud providers – SpiderOak (**https:// spideroak.com**) and Tresorit (**https:// tresorit.com**), for example – adopt this 'no knowledge' policy, but others don't.

You don't need to switch cloud provider to get this kind of protection; instead, add your own layer of encryption to critical files, with keys not shared with anyone else. An open-source encryption tool designed for cloud-based storage is Cryptomator (**https://cryptomator.org**), which works with any cloud provider from OneDrive to Dropbox. The principle is identical to VeraCrypt: You create a password-protected virtual drive – or vault – inside which your sensitive files are stored. The key difference is that Cryptomator encrypts files and folders individually, rather than as part of a larger file, so changes are smaller and quicker to upload and download.



Select "Volume Properties..." to verify the security of your drive.
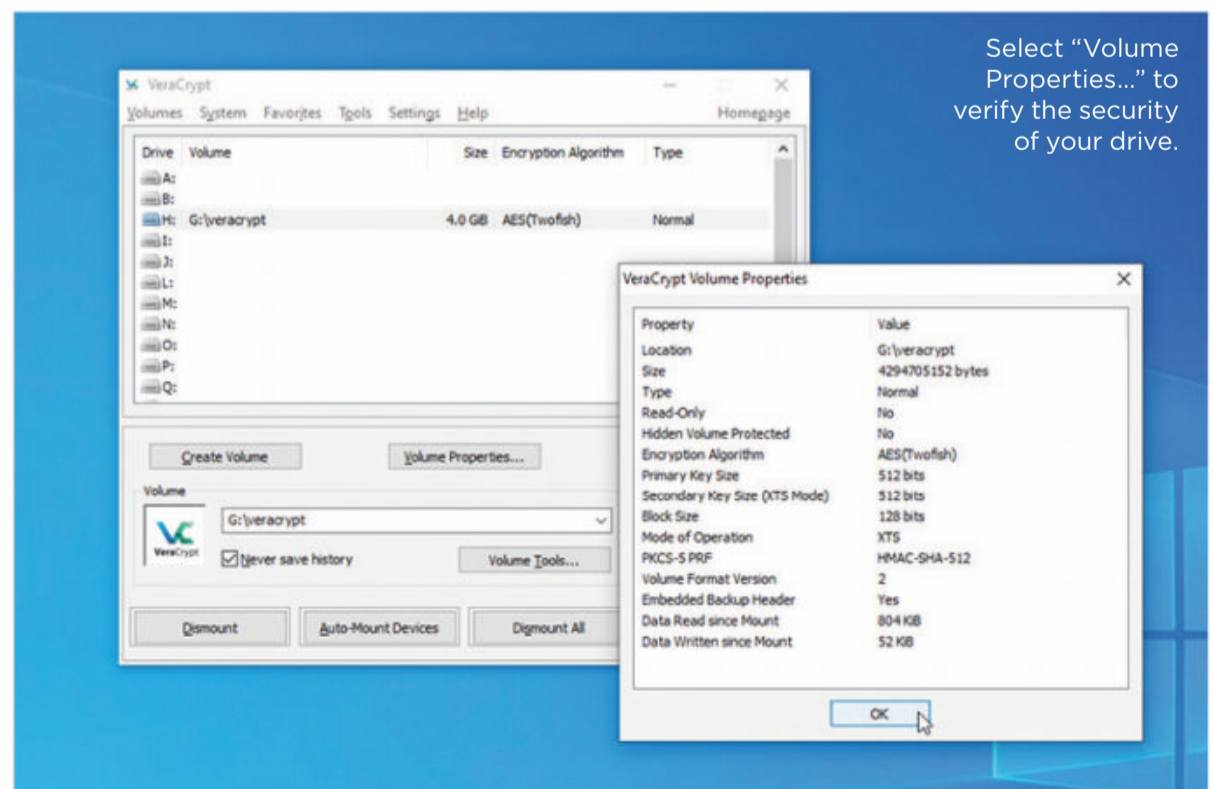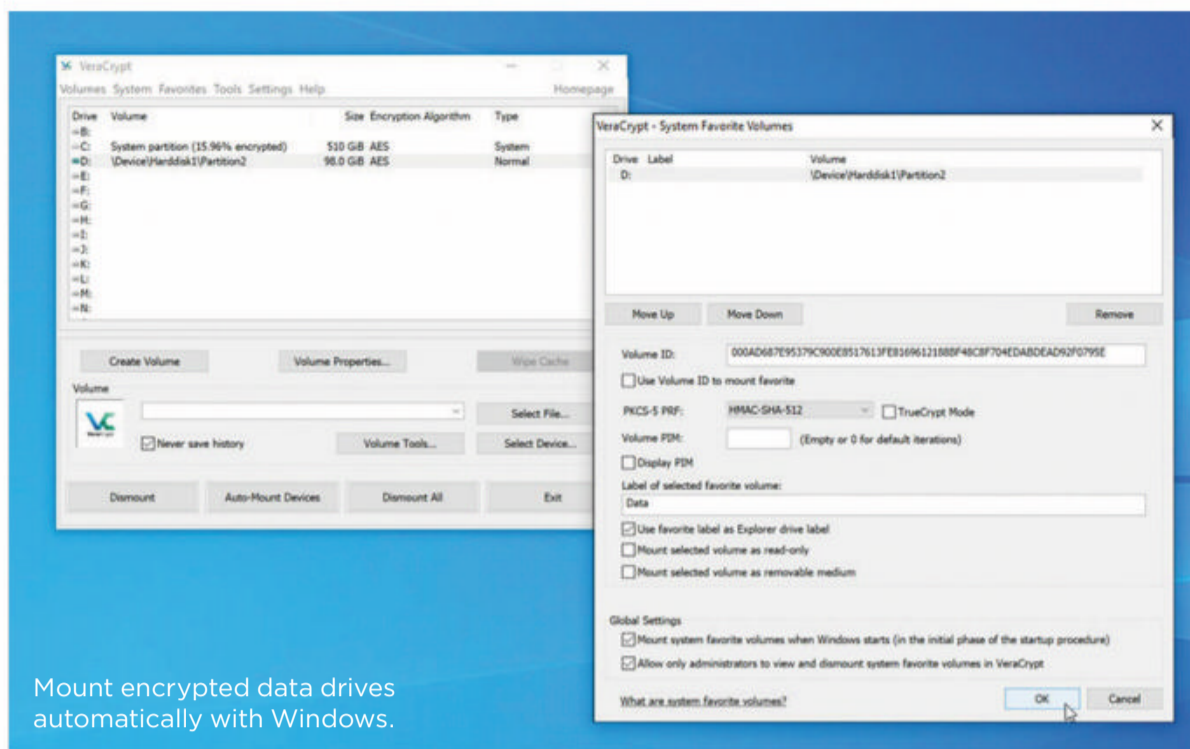
Mount encrypted data drives automatically with Windows.

## Create a container

To start, go to **www.cryptomator.org/downloads** and click Download 64 Bit. Once saved to your hard drive, double-click the setup file, and follow the install prompts, making sure you install the Dokan File System Driver when asked. Reboot if prompted.

Open Cryptomator via the Search box or Start menu, then enable the integrated update check when prompted to ensure Cryptomator stays up to date. Click the '+' button and choose Create New Vault. Navigate to your cloud folder, give your vault a suitable name (this will be the name of the folder containing your encrypted files on the drive, so don't make it too obvious), and click Save.

You're prompted to create a password to protect the vault and access it from other computers or mobile devices. We recommend generating a long random one using your password manager (store the password as a secure note). Once entered and safely recorded, click Create Vault.

Click More Options to save the password and automatically mount the drive at startup (only recommended on a secure PC). You can also change the drive name and choose a drive letter. Then enter your password and click Unlock Vault.

A new Explorer window eventually
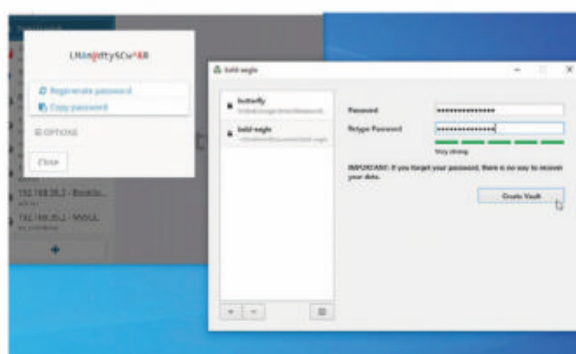

Strengthen your Cryptomator vault by using a randomly generated password.

opens, pointing to your new virtual drive (it's also accessible via This PC under Network locations) – simply copy or save files in here, and they're encrypted securely before being uploaded to the cloud.

When done, you can leave the drive unlocked until you shut down your PC or – if security is an issue – open the main window and click Lock Vault to close it down (enter your password and click Unlock Vault to bring it back later if you need to).

You can access your cloud-hosted vault from other computers by installing Cryptomator on there and choosing Open existing vault. There are even paid-for apps for Android or Apple phones if you need to upload sensitive files while on the road.

## Shortcomings

Our main gripe with Cryptomator is that its presence can't be hidden – and, in fact, is blindingly obvious to any hacker combing through your folders. That's because its master key is visible inside the folder containing your encrypted data (even the name – masterkey. cryptomator – isn't subtle). This highlights the need to keep an independent backup of any data stored in a Cryptomator vault in case these key files are damaged or lost.

If that's a deal-breaker, consider switching back to VeraCrypt, but minimise the size of your vault (make multiple smaller vaults, rather than one large one). This helps reduce the amount of bandwidth used when uploading and downloading changes to encrypted files. Another approach is to use cloud storage for encrypted file and image-based backups (see box to the right).
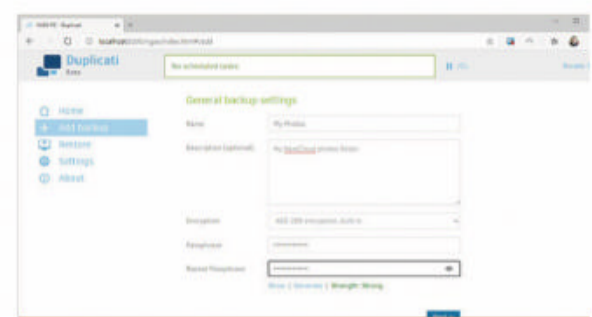
## ENCRYPT BACKUPS IN THE CLOUD

You've encrypted the files on your hard drive, but what about your backups? By default, backup tools store your files unencrypted on a local or network drive, which is fine if the drives have been encrypted with VeraCrypt or BitLocker, but what if you just want the backups to be encrypted; perhaps you'd like to store them securely in the cloud?

The answer lies with the free and open-source backup tool Duplicati, currently in beta (**www.duplicati. com**). This has been engineered like Cryptomator for the cloud, but specialises in file-based backups. After downloading and installing, let Duplicati launch – configuration is done through a browser window. Click Add backup to work your way through the backup wizard. You're prompted to set your encryption level (the default AES-256 is more than adequate) and passphrase at the start.

Next, select your destination. You can back up locally or directly to a range of cloud providers – Google Drive, OneDrive (choose the v2 option), Dropbox, and so on). If yours isn't listed, choose your cloud provider's local folder, and let its native app sync the backup files after it's been taken.

From here, select which files and folders to upload, set a schedule for updating the backup, and choose how many backups to retain. Click Save, then opt to run the backup now. A progress meter shows how far it's got – look at the throttle button if the uploading impacts your Internet performance.

When it comes to recovering files, select Restore, and follow the wizard – you can recover individual files as well as older versions of a file.

# Take great shots
## on your iPhone!

George Cairns helps you discover how to shoot, edit and share better-looking photos on your iPhone.

The iPhone is the perfect device for photographers. It's a camera that's always on hand to capture sudden photo opportunities. It's a digital darkroom packed with tools that can fix problems with color, tone, and composition. It's a portable gallery that lets you display photos on a high resolution display or share shots via social media. iPhones are also effective photography tools as they draw less attention when you're taking a photo (compared to using a bulky DSLR camera). As everybody's staring at phones these days people won't give you a second glance when you compose your shot. This low-profile provides more opportunities to capture documentary-style street photos.

Traditional DSLR photographers may look down on an iPhone because it lacks the manual controls and mechanical features that can produce particular effects. For example, a DSLR user can choose a wide aperture to create a background blur for a portrait. They can freeze a moment in time using a fast shutter speed, or add motion blur to people and cars using a slow shutter speed. And they can also instantly swap lenses to capture a wide-angle view or use a telephoto lens for a candid close-up.

The iPhone 11 and 11 Pro has narrowed the gap between iPhones and DSLRs because the telephoto and wide-angle lenses give more control over composition. Using the iPhone 11's Night mode, you can shoot in low light without a flash, and the enhanced Portrait mode lets you add a background or foreground blur to objects. Combined with the photo and video editing tools released in iOS 13, you can use your iPhone to create pro-standard pictures similar to those on DSLRs.

We used an iPhone XR and iPhone 11 Pro for this feature, but you can apply many of our tips, tricks and techniques to older iPhone models.

# Camera app options

**1** SCROLL TO ZOOM
Tap icons to jump between the iPhone 11 Pro's Telephoto (2x), Wide (1x) and Ultra–wide (0.5) lenses. Alternatively, drag the wheel to zoom in or out in increments. Up to 2x is an optical zoom. Any higher is digital zoom.

**2** PREVIEW
When using the Wide (1x) or Telephoto (2x) lenses, you'll see a faded preview of the camera feed outside of the captured area. This helps you zoom in or out (or pan to reframe) to include important details in the scene.

**3** TOGGLE MODES
Tap the arrow icon to toggle between the Camera app's shoot-ing modes (such as Slo–Mo, Video, Photo, Portrait, Pano) and other settings such as Flash controls, Night mode, Aspect Ratio, Self–timer, and Filters.

**4** SHUTTER BUTTON
Tap here to snap a shot in Photo mode or record a clip in Video mode. In Photo mode, hold the shut-ter button and slide up/right to record video. Hold the shut-ter button and then slide down/left for burst mode.

**5** LIVE PHOTO
Tap here to toggle the Live Photo mode on or off. Live Photo enables you to cap-ture a short video clip that you can process in creative ways, such as mimicking long exposure motion blur produced by a DSLR.
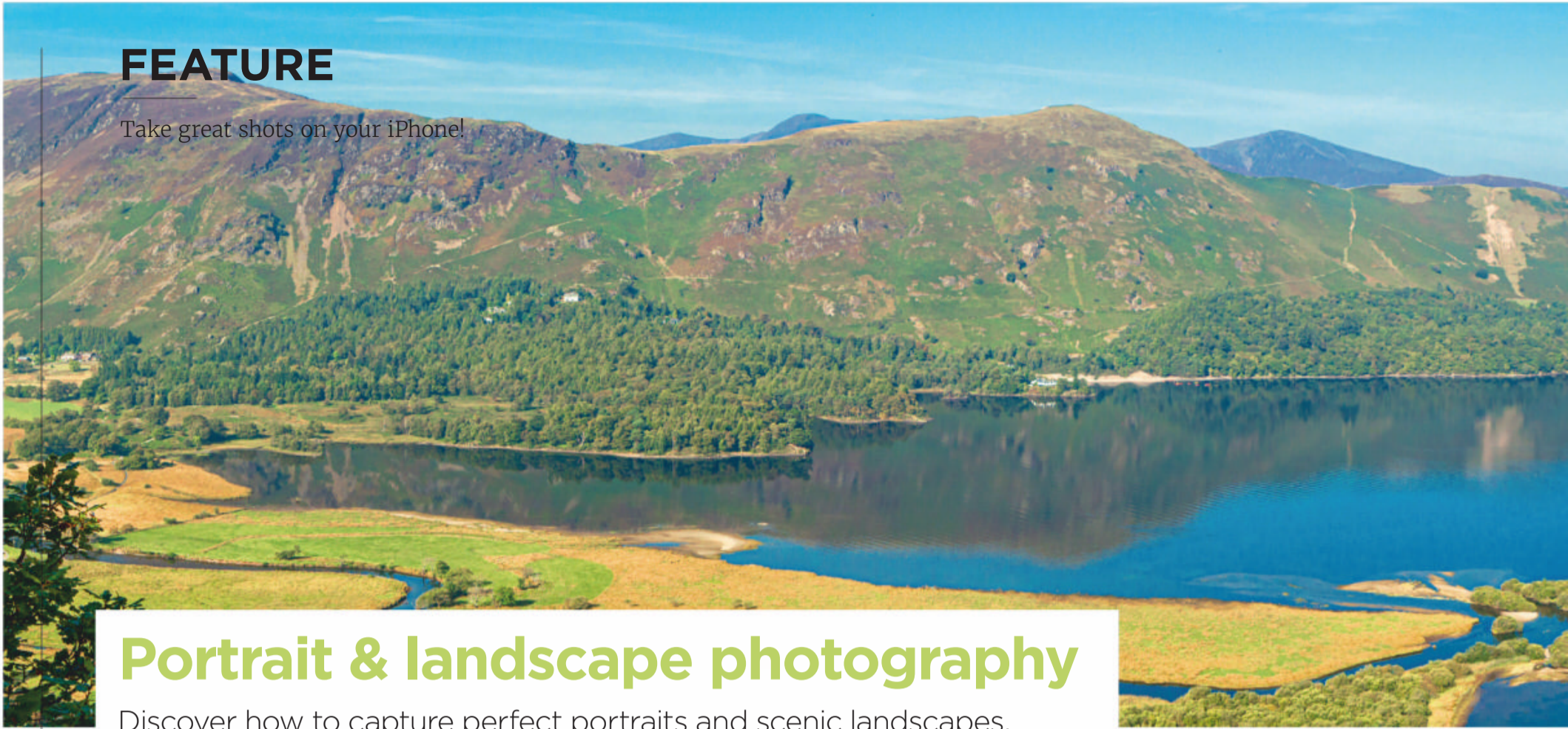
# Portrait & landscape photography

Discover how to capture perfect portraits and scenic landscapes.

People and pets are common subjects for a photograph, or you may prefer cityscapes or rural landscapes. Whatever your subject preferences, the iPhone packs all the tools and shooting modes you need. Here are some shooting tips and techniques that will help you capture the shot you're after.

### 1 Portrait mode

Digital SLR cameras have a Portrait mode that uses a wide aperture setting to create a blurred background (or bokeh). This helps complement the sharply focused subject in the foreground. The iPhone 7 Plus, 8 Plus, X and XR models also boast a Portrait mode that uses software to simulate this background blur effect, but they can only apply blur to portraits of people. Try shooting a pet and the iPhone says it can't find a face to work with. Thanks to their extra lenses, the iPhone 11 and 11 Pro's Portrait modes can apply a selective blur to any subject, making these models behave more like DSLRs.

### 2 Adjustable blur

With a DSLR, you're stuck with the strength of the background blur due to the lens's aperture setting. A wide blur-inducing aperture has a small f-stop value such as f/1.8. A narrow aperture such as f/16 will produce less blur. On the iPhone, you can use the Photos app to adjust the f-stop to dial in more blur and hide unwanted background objects, or reduce the blur to reveal more of the subject's original background. This post-production adjustment gives the iPhone more control over the final look of a portrait's bokeh effect.

### 3 Perfect panoramas

The Camera app's Pano mode lets you pan the iPhone to capture a wider field of view in a single image. By default, you need to pan the iPhone left to right to capture a panorama, but if you tap the arrow it will jump to the opposite side of the screen, letting you pan right to left. The Pano mode works best on static landscapes. If there are moving subjects they can be distorted when the panned video is stitched together into a single shot. You can also tilt the camera

## HOW TO Use different lenses

**1**

DIGITAL ZOOM On single-lens iPhones, such as the XR, pinch to zoom in for a closer view of the subject. This is just a digital zoom though, so will lack the high image quality produced by the dedicated Telephoto lens on the iPhone 11 Pro.

**2**

TELEPHOTO Tap the 2x icon to select the iPhone 11 Pro's 52mm lens. This enables you to capture a candid view of your subject without moving from your shooting spot. Perfect for shooting editorial-style stock photos and clips.

**3**

GO WIDE The iPhone 11's Ultra Wide lens can be selected by tapping the 0.5 icon. This 13mm lens is perfect for capturing landscapes and cityscapes. It creates elongated figures so is more suitable for places than people.
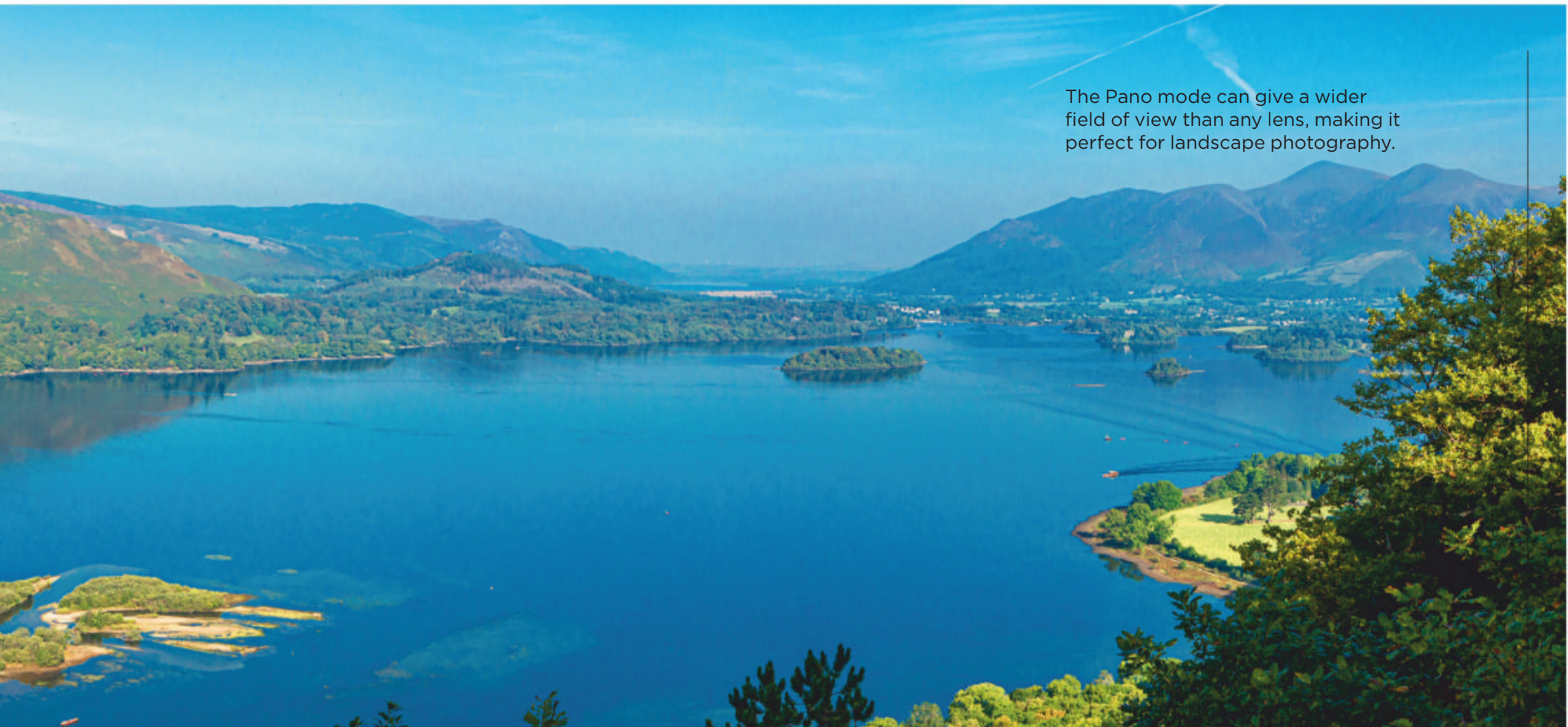
The Pano mode can give a wider field of view than any lens, making it perfect for landscape photography.

vertically in Pano mode to capture more of a tall building. This mode can also be used to capture a wider angle of view on iPhone models that lack a Wide or Ultra Wide lens.

**4** High Dynamic Range

Landscapes can suffer from high-contrast lighting. If the camera exposes to capture more highlight detail then the landscape's shadows can be underexposed. If shadow detail is captured then the brighter sky can be blown out. By setting older iPhones to HDR mode, they will snap three consecutive shots to capture detail in a landscape's shadows, midtones, and highlights. The three exposures are then composited into one shot. On the iPhone 11 Pro, you can turn on Smart HDR in the Camera Settings menu to make the Camera blend the best parts of separate exposures into a single "best exposure" shot.

**5** File formats

iPhones such as the 11 Pro can



On the iPhone 11 you can blur the background or foreground of any subject for prettier pet portraits.

save photos in the HEIC (High Efficiency Image File) format to take up less storage space. You can go to Settings > Camera > Formats and choose Most Compatible. This saves files as slightly larger JPEGs, which are easier to share online, edit in third-party apps and view on PCs.



Go to Settings > Camera > Grid to summon a Rule of Thirds grid to help you with your composition.

## Best third–party apps/Photos extensions

### Lightroom
**$14.29/MONTH**  adobe.com
Lightroom has a more advanced set of retouching tools than iOS Photos. It also boasts a camera mode that can shoot raw .DNG files. This enables you to tease out missing detail without adding compression artefacts, creating professional results.

### Halide Camera
**$9.99**  halide.cam
This app gives you DSLR–style camera settings, such as White Balance presets and manual ISO adjustment. Focus peaking enables you to see which areas are sharp. You can also AirDrop its .DNG files to your Mac and edit them in Photos.

### Shutterstock Contributor
**FREE**  shutterstock.com
After shooting a series of photos, upload your favorites to Shutterstock's stock photo marketplace via the Contributor app. It will even suggest keywords for your shots, and the review process can be very quick.

# Master low–light photography

Discover how to reveal more detail in the dark.

Shooting in low–light locations is a challenge. An iPhone can try using a faster ISO and a wider aperture to make it more sensitive to available light but this can add nasty image noise to your shots. Here are some handy suggestions for capturing better–looking photographs in low–light scenarios.

## 1 Summon the flash
One way for you to cast more light on a subject is to activate the built–in flash by tapping the Camera app's flash icon. Flash is not an ideal solution, though. A burst of flash can illuminate a person standing close to the iPhone, but it will plunge the distant background into underexposed shadow. And some locations may not permit the use of flash, such as inside a church or museum.

## 2 Use a tripod
When your iPhone meters a low–light scene it will use a slower shutter speed to let in more light. If you don't hold the iPhone still enough, you may add unwanted shake–induced blur to the image. By using a tripod, you can keep the iPhone rock–steady during the long exposure. This will cause static subjects such as buildings to look sharp. Moving subjects such as cars and people may appear motion-blurred depending on the shutter speed, which adds a dynamic sense of movement to the scene. If you have an iPhone 11 model, a tripod is not as essential thanks to Night mode.

## 3 Use Night mode
On the iPhone 11 models, you can shoot in Night mode when faced with low-light locations. This enables you to capture a handheld long-exposure while keeping camera-shake blur at bay. Night mode produces astonishingly good results, revealing details such as clouds and stars that are not as visible to the

**HOW TO** Use the iPhone 11 Pro's shooting modes



**1** NIGHT MODE Here, the yellow Night mode icon has activated automatically. It has chosen a four–second exposure to capture the scene's details. After tapping the shutter button, a countdown slider indicates the exposure time.



**2** MOTION BLUR This Night mode shot was captured with a handheld iPhone 11 Pro. Despite the slow shutter speed of 1/10 of second, the static background is sharp while the walking person displays motion blur that adds energy to the scene.
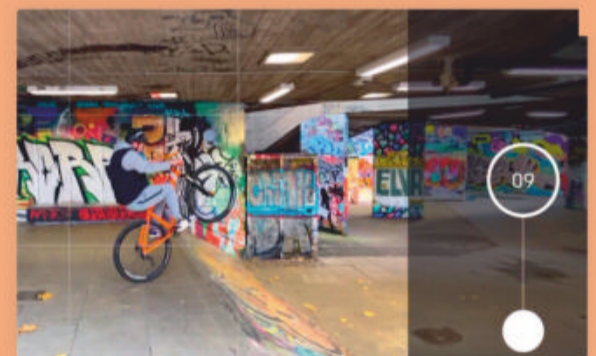


**3** BURST MODE On an older iPhone, you can capture a series of consecutive shots by holding your finger on the shutter button. On the iPhone 11, drag left (or down) to trigger Burst mode. A shot number will appear in the shutter button.

The iPhone 11's Night mode enables you to capture stunning nocturnal.

naked eye. Your Night mode shots will suffer less from high ISO speed noise.

### 4 Read the metadata

To understand the settings that the iPhone uses in low–light locations, click on a picture in your Mac's Photos app. Click the "i" icon at the top right. This opens a metadata panel that provides you with the photo's shooting settings such as ISO (sensitivity to light). The higher the ISO speed, the more sensitive to light your iPhone will be. A high ISO speed such as 2,000 will add ugly particles of picture noise to your low–light shot. When faced with a high ISO speed shot, click on Edit

and use the Noise Reduction slider to smooth out the noise.

### 5 Shoot in raw

Photo file formats such as HEIC and JPEG compress an image so that it takes up less space. This makes it harder to reveal color and detail in low–light shots. With an uncompressed image, such as a .DNG (Digital Negative), you can restore missing detail without revealing as many nasty compression artefacts.



**4** PORTRAIT MODE The Portrait mode's shallow depth-of-field blur isn't re-stricted to portraits of people or pets. You can use it to add bokeh blur to other subjects. Here we used Portrait mode to draw attention to the fore-ground ivy.



**5** HIGH-KEY MONO The High-Key Light Mono setting uses the depth mask created in Portrait mode to isolate the subject from their background. This is a quick way to simulate a high-contrast monochrome studio photo in any location.

## Best iPhoneography accessories

### Mini Tripod

**$75**  manfrotto.com

This mini tripod and universal iPhone clamp enables you to capture rock–steady clips and Live Photos. Its small size gives you dramatic low–angle shots. It's also great for capturing motion blur during long exposures.



### LED Light Lumimuse

**From $179.95**  manfrotto.com



The LED Light Lumimuse enables you to light your photo or video subject from an angle and reveal more detail in low–light locations. The light comes in 3, 5 and 8 LED brightness options, and you can adjust the intensity of the light.

### Muvi X–Lapse

**$39**  veho-world.com

On a tripod, your iPhone can capture stunning time–lapse clips that show the ebb and flow of people or clouds at high speed. This clockwork tripod rotates very slowly, adding a smooth pan to your time–lapse clips.

Selectively adjust a backlit subject to reveal missing shadow and highlight detail.

# Master image/video-editing

Get your photos and clips looking their best.

After shooting a photo or capturing a clip, you may need to tweak its color, tone, and composition to improve it. Fortunately, iOS 13's Photos app boasts a powerful digital darkroom to counteract common problems. It can also process footage using the same tools, helping clips to make the grade.

## 1 Tints and casts

Your iPhone needs to capture true colors under various lighting conditions. This can be a challenge due to the different color temperatures of light. Daylight can cause a shot to look too cold and blue. Artificial light can make skin tones look too warm and orange. Your Camera app will perform an Auto White Balance

(AWB) operation to capture cast–free colors. If it can get white objects to be free of blue or orange casts, the rest of the image will have cast–free colors too. If your shots still suffer from color casts you can counteract these in the Photos app. Tap Edit, then tap the Adjust icon and swipe to the Warmth slider. Drag it left to warm up a cold blue shot or right to cool down a warm orange cast. You can also remove green or magenta color tints using the Tint slider. Drag it left to counteract a green tint or right to reduce magenta. These fixes will work with stills or clips.

## 2 Tonal tweaks

In contrasting lighting conditions, your

iPhone may struggle to capture detail in the shadows and the highlights (even when shooting an HDR image). The Adjust panel's Shadows slider enables you to lighten underexposed shadows without overexposing highlights. The Highlights slider claws back any missing sky detail without underexposing a darker landscape.

## 3 Distortion

If you shoot a tall building from a low angle its vertical walls appear to converge inwards towards the top of the frame. This phenomenon is called perspectival distortion. If you use an Ultra Wide lens, you'll want to embrace this perspectival distortion as a feature

## HOW TO Edit Live Photos in iOS 13

**1**

SHOOT IN LIVE MODE After shooting in Live mode, hold your finger on a Live Photo to play a three-second movie. Live Photos can be edited in the Photos app to choose the best frame, adjust colors and tones, and even create animations.
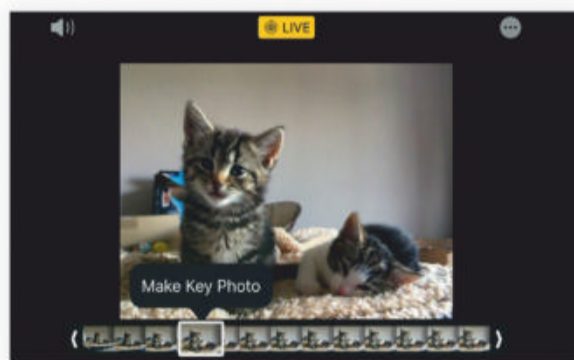
**2**

SET A KEY FRAME  Tap Edit, then tap the Live icon. Trim the start and end point of the Live Photo. Drag the white rectangle to choose the best frame. Tap Make Key Photo to display this frame as the Live photo's thumbnail.
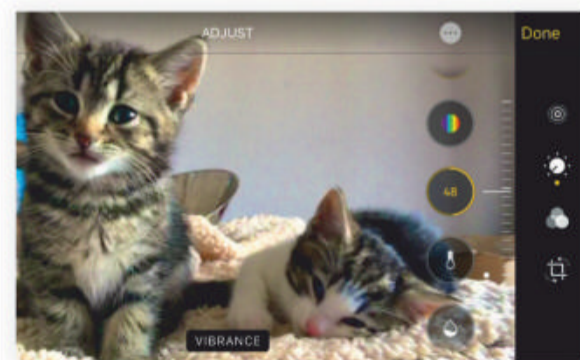
**3**

ADJUST CLIP Tap the Adjust icon and tweak colors and tones to make the clip look its best. Here we have increased the Vibrance amount to boost the saturation of the Live Photo's weaker colors without oversaturating stronger ones.

The Photos app lets you apply filters either before or after you shoot to help you create a specific look.

of wide–angle photography. However, when using other lenses you can process the picture to make the walls of a building run parallel with the side edges of the frame. Tap Edit, then tap the Crop icon. Tap the Vertical correction icon. Drag the slider right to reduce vertical perspectival distortion.

### 4 Fun with filters

The Camera app's Filter icon enables you to quickly grade a photo or clip's colors and tones to produce a wide range of looks in seconds. Nine thumbnails act as springboards to create striking effects such as Vivid Warm or Dramatic Cool. You can also produce high–contrast mono effects such as Silvertone. The strength of each filter can be dialled down to achieve a more subtle look.



Tap the F icon then dial in more (or less) background blur.

## Sharing images on social media and elsewhere

After processing your pics, you may want to share them with friends, family, and social media followers. Some social media sites will present a cropped version of your shot. For example, if you share a portrait photo on Twitter, it may be presented in a landscape box that cuts off key parts of the image. Consider cropping a portrait shot as a landscape shape in Photos. Tap Edit, then tap Crop and check the landscape icon. Drag inside the crop window to reframe the subject. Tap Done. Tap Share, then tap your chosen social media app's icon.
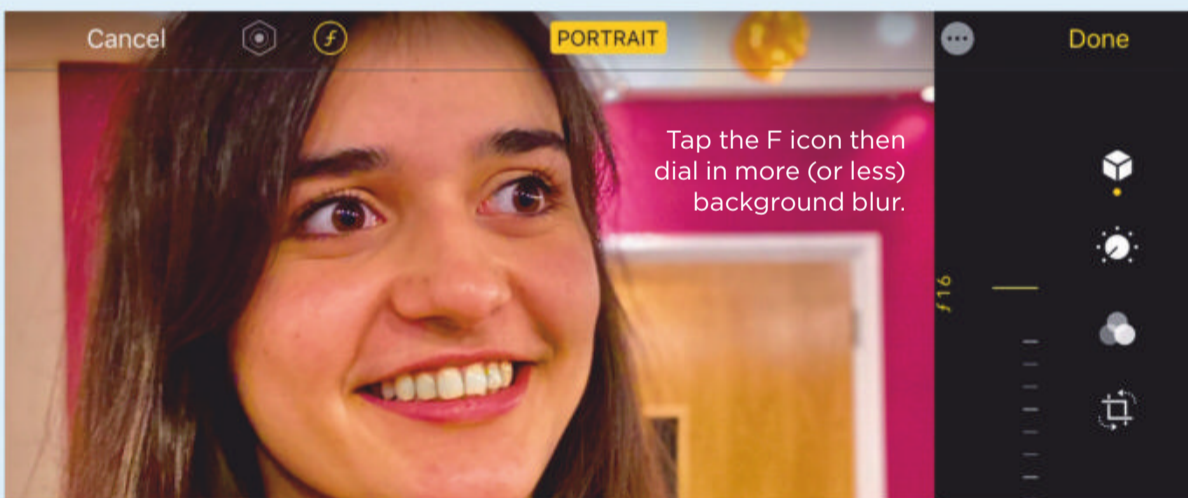


Crop a shot so that key areas will display in your Twitter feed.
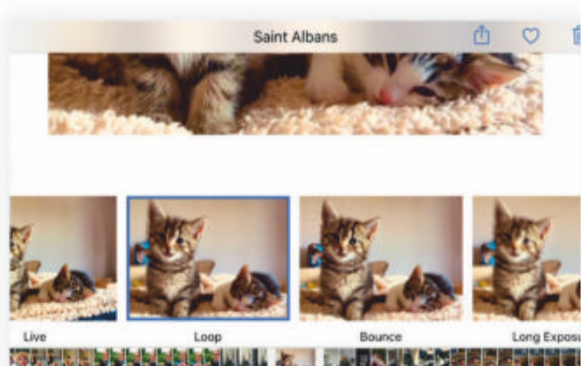


**4**

ANIMATE THE CLIP When viewing a Live Photo, swipe up to access its animation tools. Loop plays the clip then mixes it back to the start. Bounce works well with animals as it plays the clip backwards and forwards to create repetitive movement.
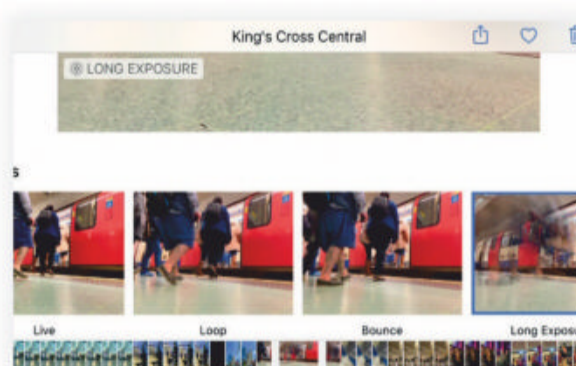


**5**

SLOW SHUTTER EFFECTS On a DSLR camera you can close the aperture and use a slow shutter speed to add motion blur to moving people or objects. You can mimic this technique by applying the Long Exposure animation to your Live Photo.



**6**

LONG EXPOSURE We shot this Live Photo on a tripod so only the people would move. The Long Exposure effect blurred the moving people while keeping the train looking sharp. This technique can turn ocean waves into abstract foamy streaks. **TL**

# Free up space on your PC

How can you ensure your PC doesn't run out of storage? Nick Peers has some pointers…

"You have run out of disk space." There it is, unequivocal. It wasn't that long ago that Windows started popping up "You are running out of disk space" messages, swiftly followed by "You are running very low on disk space." No matter, the day has finally arrived. Your hard drive has finally run out of space, and now you have to do something about it. The question is: What?

These days, running out of disk space should be impossible. With terabytes of storage available to you, how do you manage to fill it all up? One reason might be that you don't actually have terabytes to start with – perhaps you're using a laptop that only came with 128GB, or a two-in-one tablet whose 32GB is barely enough to fit Windows on, never mind any apps or data.

Don't panic, though, because over the next few pages, we show you everything you need to know to solve the problem. You'll learn to spot the early warning signs, plus take steps to keep your hard drive as clean as possible. We also examine ways to add extra capacity, enabling you to move your data off your boot drive to free up space. And if all else fails, we show you how to upgrade your PC's boot drive, plus migrate everything from the old to the new drive. It's all here, so turn the page to solve your disk space issues.

# Monitor your drive space

Find how what happens when you run out of free space, and how to keep an eye on how much is left.

That warning we flagged in the intro is unlikely to be the first indication you get that you're running out of space. It's not designed to appear until you have 200MB or less free – a drop in the ocean these days. Instead, Windows' first warning is likely to appear when you open File Explorer to the "This PC" view to see your drive's usage is represented by a red bar, rather than a blue one. This appears when your drive has less than 10 percent of its space left, although the seriousness of the warning does depend on the size of the drive. For example, a 64GB drive with under 6GB left is more worrying than a 2TB drive with 180GB free.

## More drive alerts

Windows Update also throws up an alert if it discovers there's insufficient room to install the latest updates – this usually appears when you don't have secondary storage attached to your PC for it to use as temporary storage. It can pop up when there's as much as 11GB still free on your drive for major updates, but of more concern is if it shows when you're trying to install a cumulative update, which indicates your drive has less than 3GB left.

All PCs make use of small recovery partitions (anywhere from 500MB to 8GB). Sometimes, these partitions are assigned drive letters in Windows – often in error. Because they're designed to store specific files and nothing else, they can be filled almost to capacity, resulting in Windows throwing up a low space disk warning.

The solution is simple: Type "disk" into the Search box and click "Create and format hard disk partitions." Locate your Recovery partition in the list, then right-click it, and choose "Change Drive Letter and Paths." Click "Remove" followed by "Yes" at the warning, and finally "OK." Bingo – no more warnings for that drive.

## Monitor disk usage

It's all very well knowing that your free space is disappearing, but what's actually taking up all that room? Your first stop on the quest for knowledge should be Windows' own tools: Navigate to "Settings > System > Storage," and after a short while, Windows reveals what types of file are taking up the most space on your system drive. You'll see categories for "Apps & features" and "Temporary files," and you can click "Show more categories" for a more precise listing of usage by categories as varied as "Mail," "Documents," and "Videos."

Click an entry in the list, and you're able to not just view more detail, but take remedial action. For example, if your Temporary files are gobbling gigabytes of space, click this to manually clean them up – note, the Temp setting now covers files stored in your "Downloads" folder, although they are excluded by default. As you'll see over the page, you should make use of Windows' new Storage Sense feature to manage this automatically, removing temporary files as required to prevent your computer from running low on disk space.

Although Windows has an "Other" view to cover large folders, it's not capable of easily highlighting the

> *All PCs make use of small recovery partitions, from 500MB to 8GB.*

## A different view

If you don't like WinDirStat, and are looking for a different approach to viewing your drive's make-up, try SpaceSniffer (**www.uderzo.it/main_products/space_sniffer**). It has a more modern user interface, but more importantly provides a visual view that helps you identify which folders contain the most files. Again, be sure to run it as an administrator. Unlike WinDirStat, you must focus a view on one drive at a time, but thanks to its labeling system, it's easier to spot which folders contain the most data, as they're clearly named, and their file size listed. Simply double-click one to zoom in to view its contents, or double-click its parent folder (displayed above it) to zoom back out.

If you know which files are likely to take up most space, use the "Filter" box to input a file type (such as *.mp4) and click "Filter" to focus on that. Right-clicking a displayed folder brings up the File Explorer context menu, enabling you to delete unwanted files.
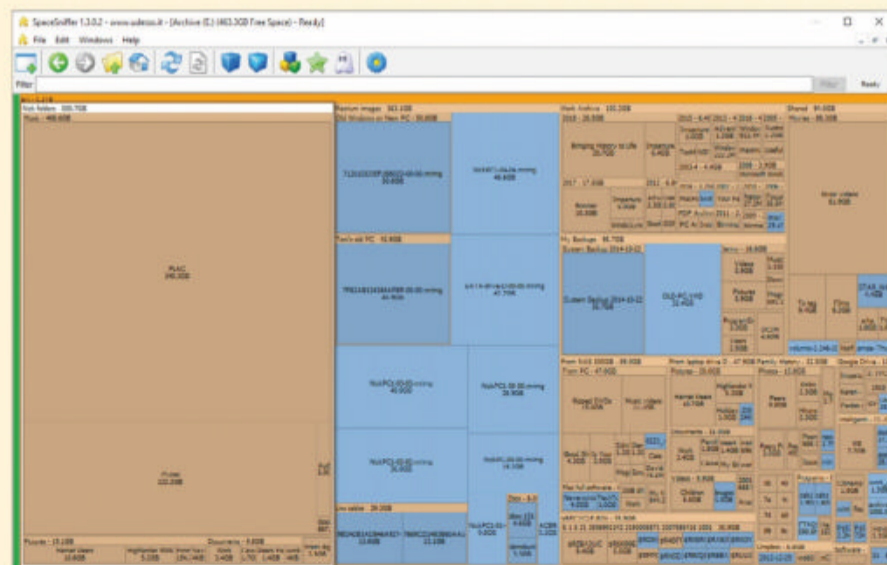


Tree-mapping is a method of displaying hierarchical data, such as the folder structure on a large hard drive, in a logical way, making it easy for a human to understand.
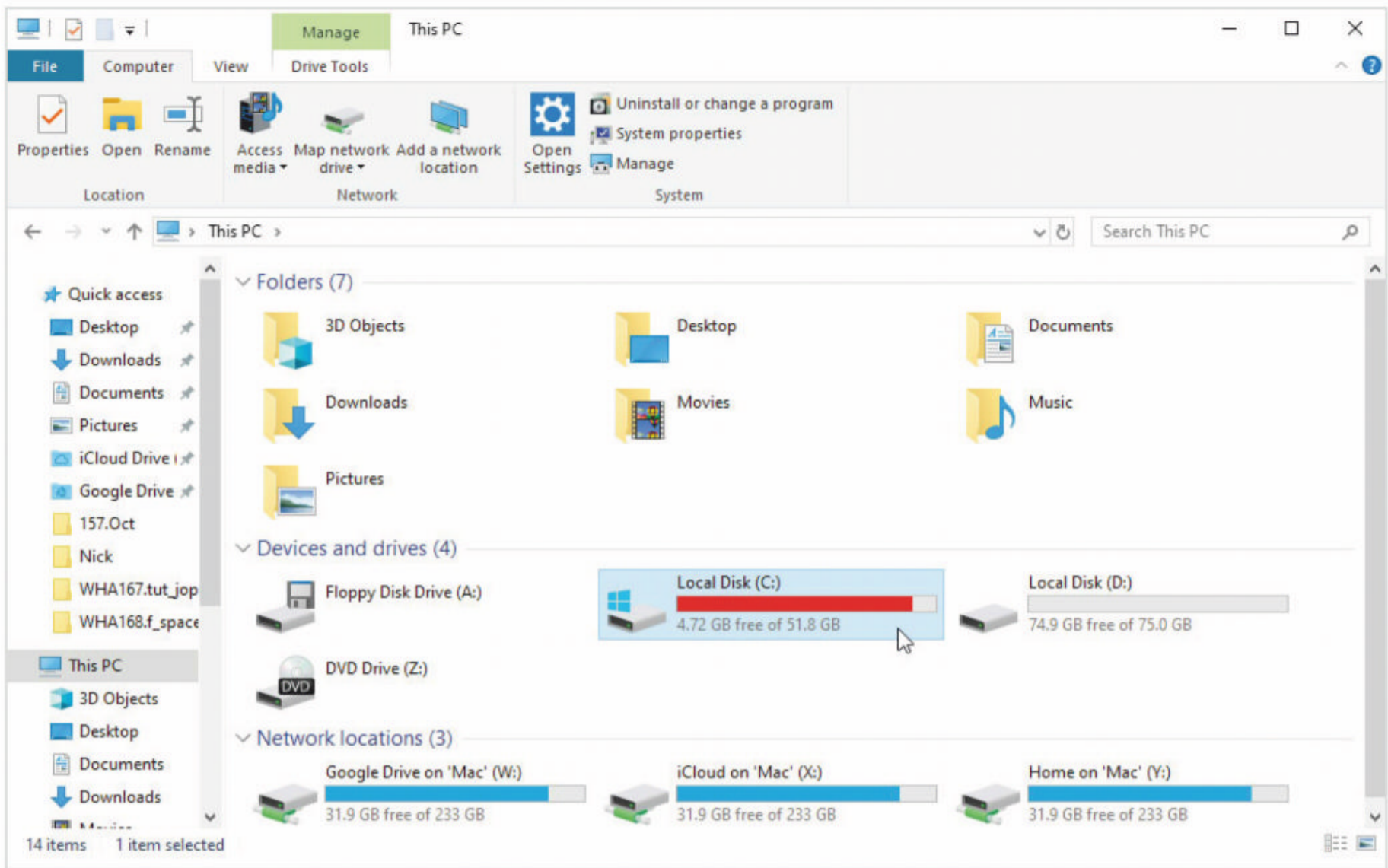
A red bar indicates that less than 10 percent of that drive's space remains free.

individual files and folders that are taking up the most space. To search for these requires a third-party tree-mapping app. Tree-mapping tools provide a visual representation of each file on your hard drive(s) in the form of blocks, with the size of each block corresponding to the size of the file in question.

One such free tool is WinDirStat

(**https://windirstat.net**), which you can download and install from its parent website or add to your PortableApps toolkit for running on demand. To add it to your toolkit, open the PortableApps platform and click "Apps > Get More Apps > By Category" – you'll find WinDirStat in the "Utilities" section. Once installed, right-click the program shortcut and choose "Run as administrator" to allow it

to check your entire drive, then see the step-by-step guide below to find out how to use it to target and – if necessary – delete individual files. Check out the box below-left for an alternate tool should WinDirStat's garish interface put you off.

Once you've determined where all your drive space has gone, you can decide how to tackle the issue. So, turn the page….

## Monitor disk space with WinDirStat
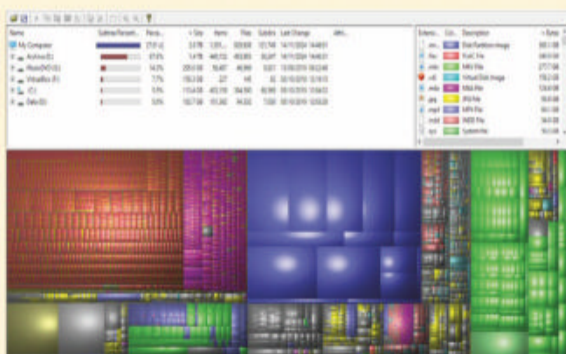


**1** VIEW A SUMMARY You can choose to monitor all drives or focus on a specific drive. Make your choice and click "OK." Wait for WinDirStat to finish its analysis and you'll see a three-paned window. The bottom provides a color-coded "map" of your hard drive according to how it's being used.
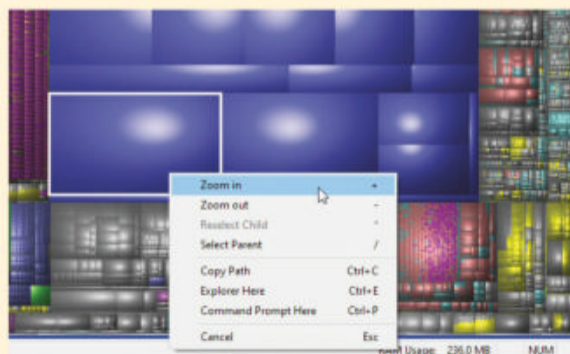


**2** INVESTIGATE IN DETAIL Click an item on the map and its filename and path are revealed in the top-left pane, which shows a traditional folder view. Right-click and choose "Zoom in" to view a map of the next level down: either a specific drive or the folder containing your target file.
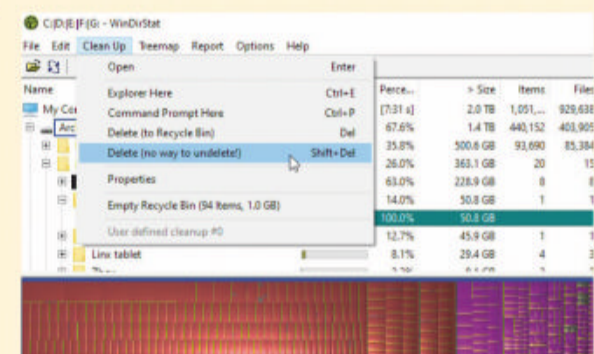


**3** REMOVE LARGE FILES When you've identified a file you think is safe to remove, select it and open the "Clean Up" menu. You can delete it directly from here or choose "Explorer Here" to open a File Explorer window pointing to the parent folder, enabling you to examine it more closely.

# Clean Up Your PC

Before buying more, ensure you're not wasting the storage you have.

Freeing up space on your PC has never been easier, thanks to Windows 10's new Storage Sense feature, which is designed to render third-party apps such as CCleaner redundant. Your first job, therefore, is to employ its services to free up additional space on your drive. Navigate to "Settings > System > Storage," and click the "Configure Storage Sense or run it now" link. Flick the Storage Sense switch on and choose when to run the disk-cleaning tool – by default, it runs when you get low on disk space, but if you want to take a more pre-emptive approach, you can run it monthly, weekly, or even daily.

Scroll down, and you can configure more options – for example, removing temporary files, emptying files from the Recycle Bin after a set period, and periodically cleaning out the "Downloads" folder. You can also configure OneDrive's on-demand feature so that downloaded content reverts to online-only if unopened for 1, 14, 30, or 60 days. Desperate for more space? Click "Clean now" to perform a one-time clean-up.

## Files on demand

If you're a Microsoft OneDrive user, chances are you're already taking advantage of a relatively recent feature known as "on-demand." Instead of keeping everything physically stored on your computer, a series of shortcuts is created instead, pointing to the online files. These take up a fraction of the space, while ensuring your files are always accessible (so long as you're connected to the Internet). Simply open a file in the normal way, and it's downloaded to your computer, kept there indefinitely, or – if configured as outlined above – until the file hasn't been touched for a set period, at which point it reverts to being online-only to free up space on your PC until you next open it.

To verify the feature is on, right-click the OneDrive icon and choose "Settings > Settings tab," then check "Save space and download files as you use them."

## Track down duplicates

It's amazing how easily we generate copies of files – or near-duplicates, in the case of digital photos, with multiple attempts to get the perfect shot all somehow being left on your hard drive at the end of the process. In the past, we've looked to Duplicate Cleaner Free (**www.digitalvolcano.co.uk/ duplicatecleaner.html**) and AntiDupl (**https://ermig1979.github.io/AntiDupl/ english**) to cover these bases for free. The Pro version of Duplicate Cleaner – US$29.95 – can also hunt out similar files, but before investing, why not give AntiTwin (**www.joerg-rosenthal.com/ en/antitwin**) a go?

Despite not having been updated since 2010, this no-frills tool works perfectly in Win 10 and can cover all your bases, as the step-by-step guide opposite reveals. Your selections are clearly marked before you commit to anything, and when you click to delete, you're given the option of moving files to a folder on the same drive for transferring elsewhere, sending them to the Recycle Bin, or deleting them directly.

Look, too, for the option to replace the file with a symbolic link to the file you've kept – this means a program referencing the file you've deleted will be redirected to the remaining file instead, ensuring it continues to work correctly.
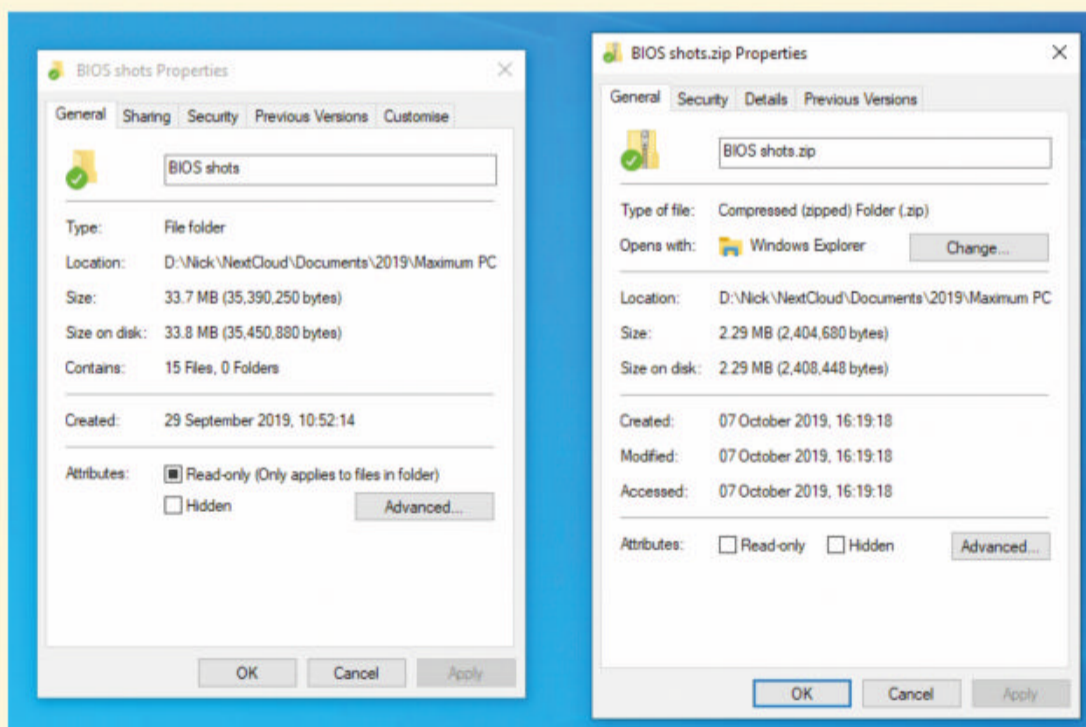


### Archive old files

Another way to save space is to move folders and files on to a secondary storage drive, such as a USB drive. If you don't have this luxury, you can save space by zipping up these rarely used files and folders instead. Right-click the item(s) in question, and choose "Send to > Compressed (zipped) folder," then wait for it to be combined into a single zip file. Right-click this and choose "Properties," then compare its size to the original file. If there's a significant saving, delete the original file or folder, then repeat to keep freeing up more space.

# HOW TO Remove duplicates with AntiTwin
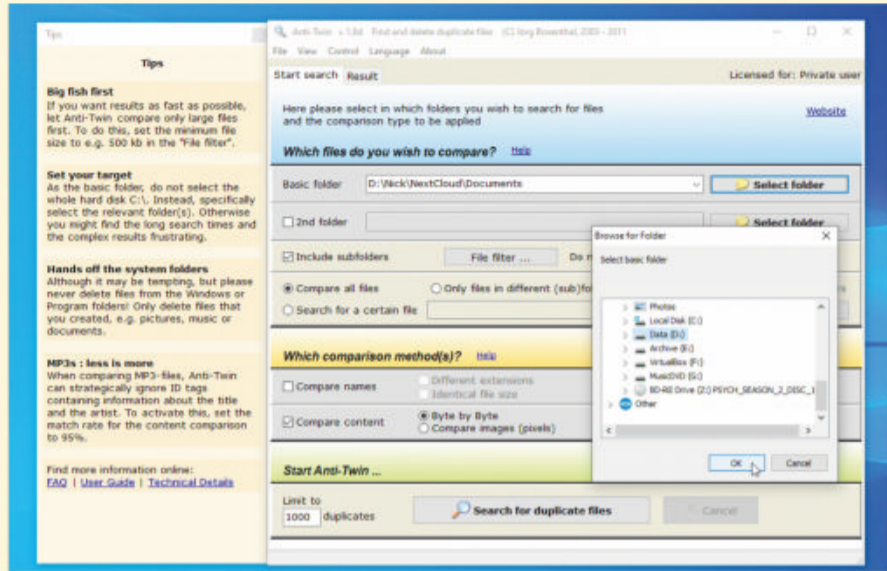


1 SELECT HARD DRIVE Open AntiTwin. Click "Select folder" next to "Basic folder" to select the root of your drive if you're looking to clear up space on one drive only. Check "2nd folder" to select another folder path or drive if you're looking to clear space across two hard drives by weeding out duplicates.
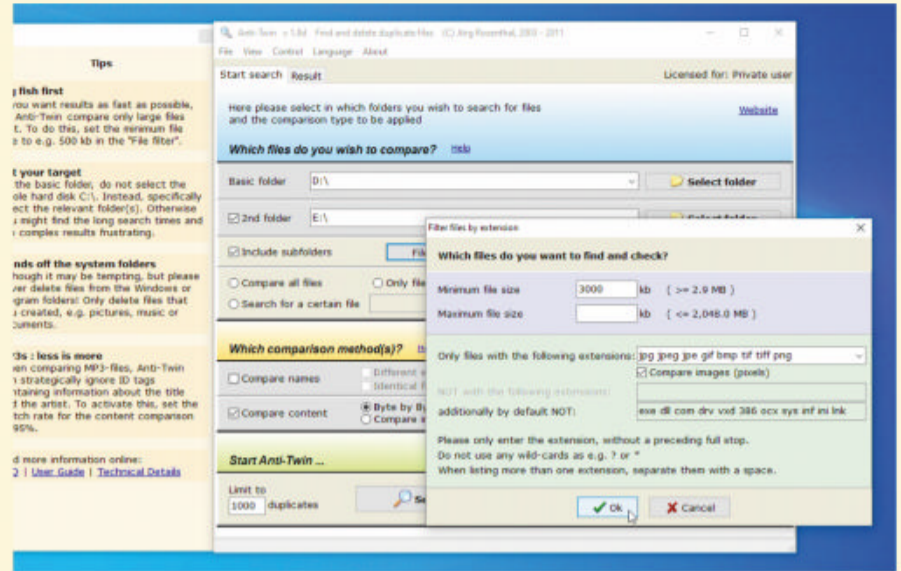


2 FOCUS SEARCH Leave "Include subfolders" checked and click "File filter." You can exclude smaller files from the search (and speed it up) by setting a minimum file size. Click the drop-down as shown to focus on specific file types, and check "Compare images (pixels)" to look for visually similar images.
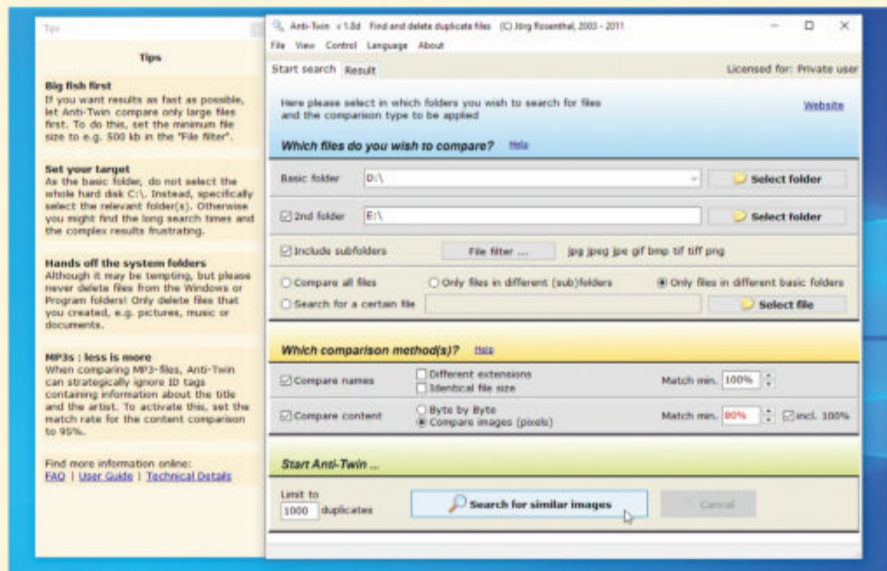


3 PICK YOUR COMPARISON METHOD By default, files are compared according to their content only, but you can also compare by name and file size if you wish. The "Match min" figure enables you to match similar, but not identical, files—this is best left for image searches only. Once done, click "Search."
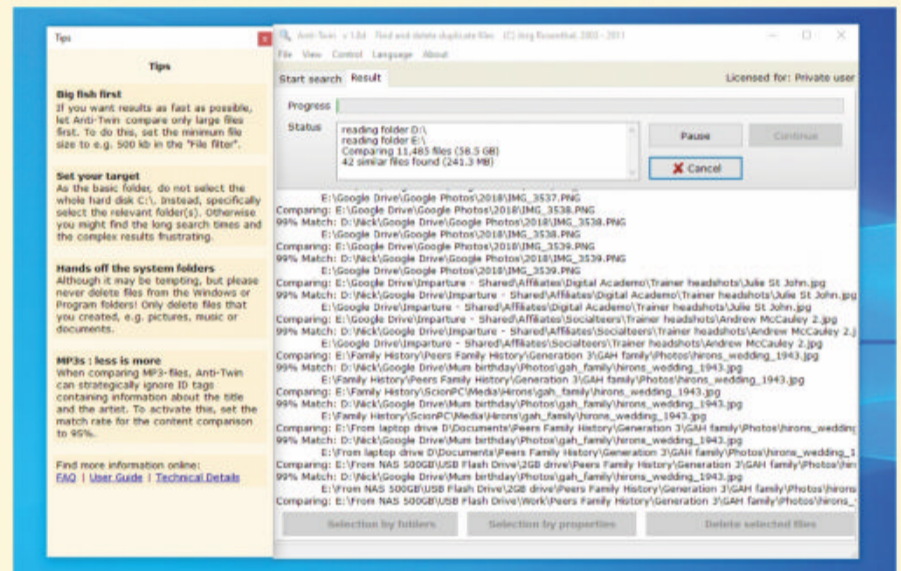


4 WAIT FOR SCAN A progress window appears – don't be surprised to see it freeze occasionally as files are checked. You can pause or cancel the search at any time. After the folder contents have been read, files are compared to see which are duplicates and (if selected) close matches.
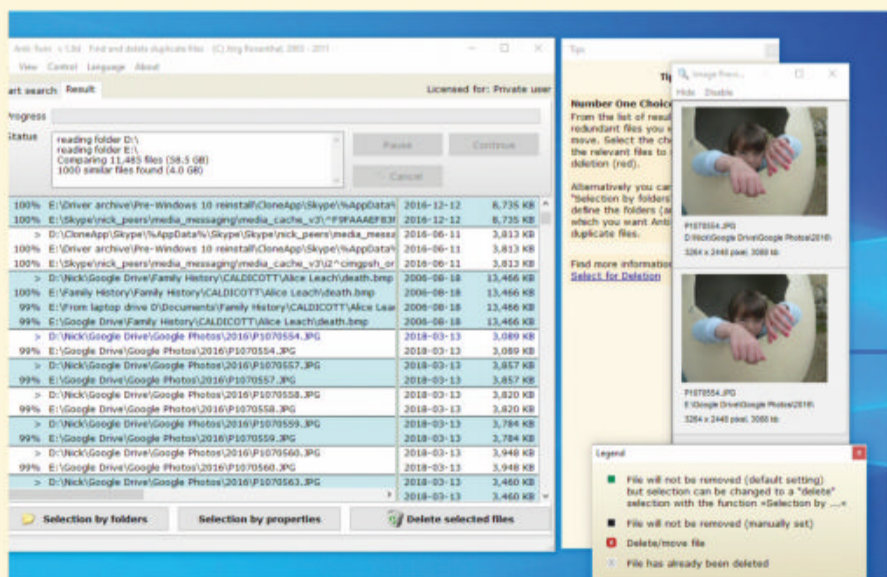


5 REVIEW RESULTS If you chose two paths, read the warning, but click "OK" as this would only be an issue if they were both pointing to the same folder. A list of all duplicates and similar files is shown, grouped together. Images can be compared by selecting one to reveal a pop-up window.
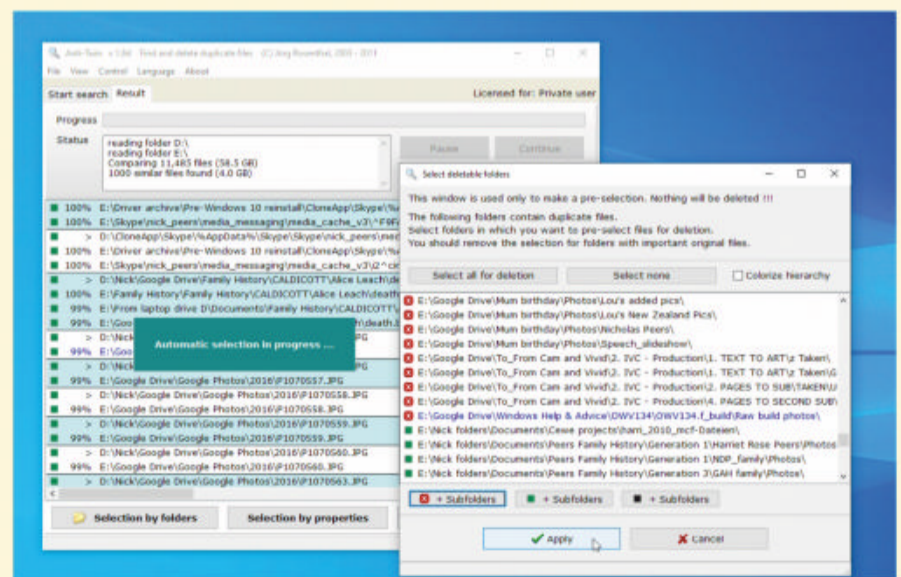


6 REMOVE DUPLICATES Right-click a file to decide whether to keep or remove it – you'll also see options that enable you to mark specific folders as duplicates (see main text). After making your selections, use the legend to verify you've picked the right files to delete before clicking "Delete selected files."

# Move your files

Transfer files elsewhere – on to another drive or into the cloud.

The march of technology leads to increased demands on your system, particularly if you've discovered a space-hungry hobby such as gaming or 4K video editing. If you're simply looking to expand available storage for your files, you have two basic options. The first is to buy additional storage. Desktop users can check whether their PC case has room for a second internal hard drive – with 4TB drives at under $200, you can solve all but the most demanding needs with a single purchase.

Before splashing out, power down your PC, open the case, and verify there's a spare drive bay. Also, check your power supply has a spare SATA power socket (if not, Google "molex to sata power adapter" to find a cheap adapter) and a spare SATA slot on the motherboard. You also need a SATA data cable – these can be had for under $1, but ensure it's SATA III (6Gb/s), and consider a right-angled connector on one end for hard-to-reach sockets.

## Other upgrades

An internal hard drive is better than an external model for reasons of speed, but this isn't always practical – for example, if you have a laptop. External drives may be more suited to long-term storage such as backups or archiving, but they can at a pinch be used for day-to-day use, although it's still a good idea to keep frequently accessed files on your internal drive.

If you want to go down the external drive route, you have two options: USB or NAS. USB prices are incredibly competitive – slightly cheaper, in fact, than internal models—so you can pay $150 (or less!) for 4TB or push the boat out and get 6TB for not much more. All models should now be USB 3.0, so for best performance, be sure to plug them into a USB 3.0 port (typically marked in blue) on your PC. Expect to pay a small premium for smaller, laptop-friendly 2.5-inch external drives, or consider network attached storage (NAS) instead. These solutions are slower, but use your network connection, so may be a more practical alternative should you not wish to have your laptop permanently connected to a USB drive.

Once your new drive is set up, you'll want to transfer your data across – the guide below-right reveals how to do this for all your user folders, which are where the bulk of your data is.

## Move some apps

If you're running Windows on a very small boot drive – say 32GB – it's not enough to move data off your system drive, because you'll quickly run out of space for new apps, too. Where it's not possible to upgrade your system drive for a larger model (see over the page), you can also investigate ways of moving your programs from your system drive to your data one. One caveat: In most cases, your new data drive will be slower than your Windows drive, particularly if you boot from an SSD, so be prepared for a performance hit, and try to keep those apps you use most often on your boot drive.

There are two ways to move apps to a new drive: First, Windows Store apps (including those pre-installed with your PC, such as Photos) can sometimes be moved via "Settings > Apps > Apps & features." Click the app in question and look for a "Move" button – if it's not grayed out, click it, select which drive to move it to, and finally click "Move" again.

Regular programs are so well integrated into the operating system that you can't simply move their folder

## Into the cloud

Another storage location you can use is your cloud provider. We've seen how you can use OneDrive to free up space on your PC, and other providers offer similar features in their paid-for plans – Dropbox (**www.dropbox.com**) calls its equivalent Smart Sync. You need to navigate to a folder inside your Dropbox folder, right-click it, and choose "Smart Sync > Online-only," or go to "Preferences > Sync," select your account, and choose "Online-only" to make it the universal default.

If you'd like to access Google Drive or Dropbox folders in this way without a paid account, for a one-off fee (US$39) you can use a tool called Mountain Duck 3 (download a free trial from **https://mountainduck.io**). This can create a series of virtual drives connecting to a range of online storage services, and supports on-demand access like that found in OneDrive across all connected services. Set "Connect Mode" to "Smart Synchronization" the first time you add a new cloud account.
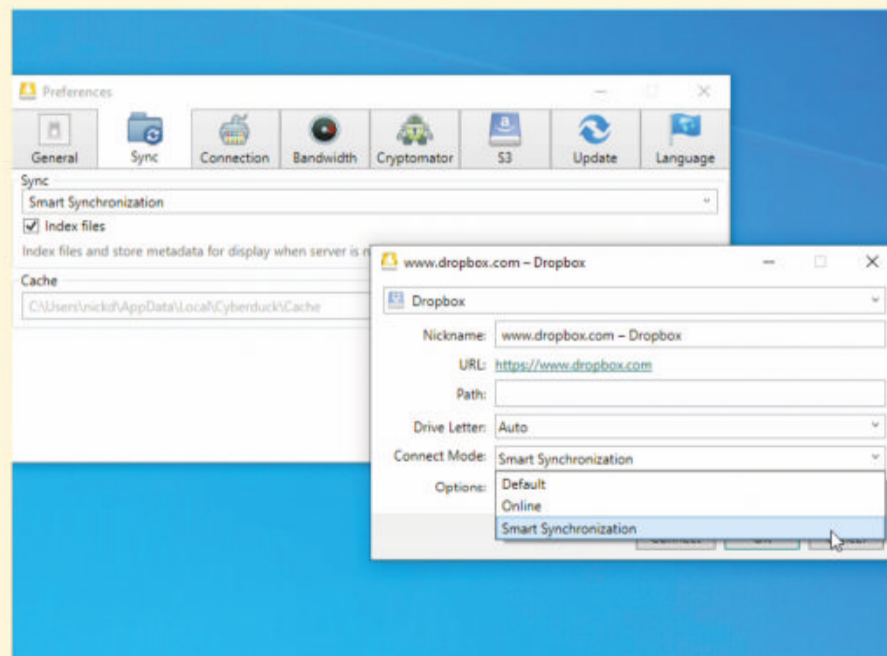


Mountain Duck mounts cloud storage as virtual drives, with files kept online to save space.
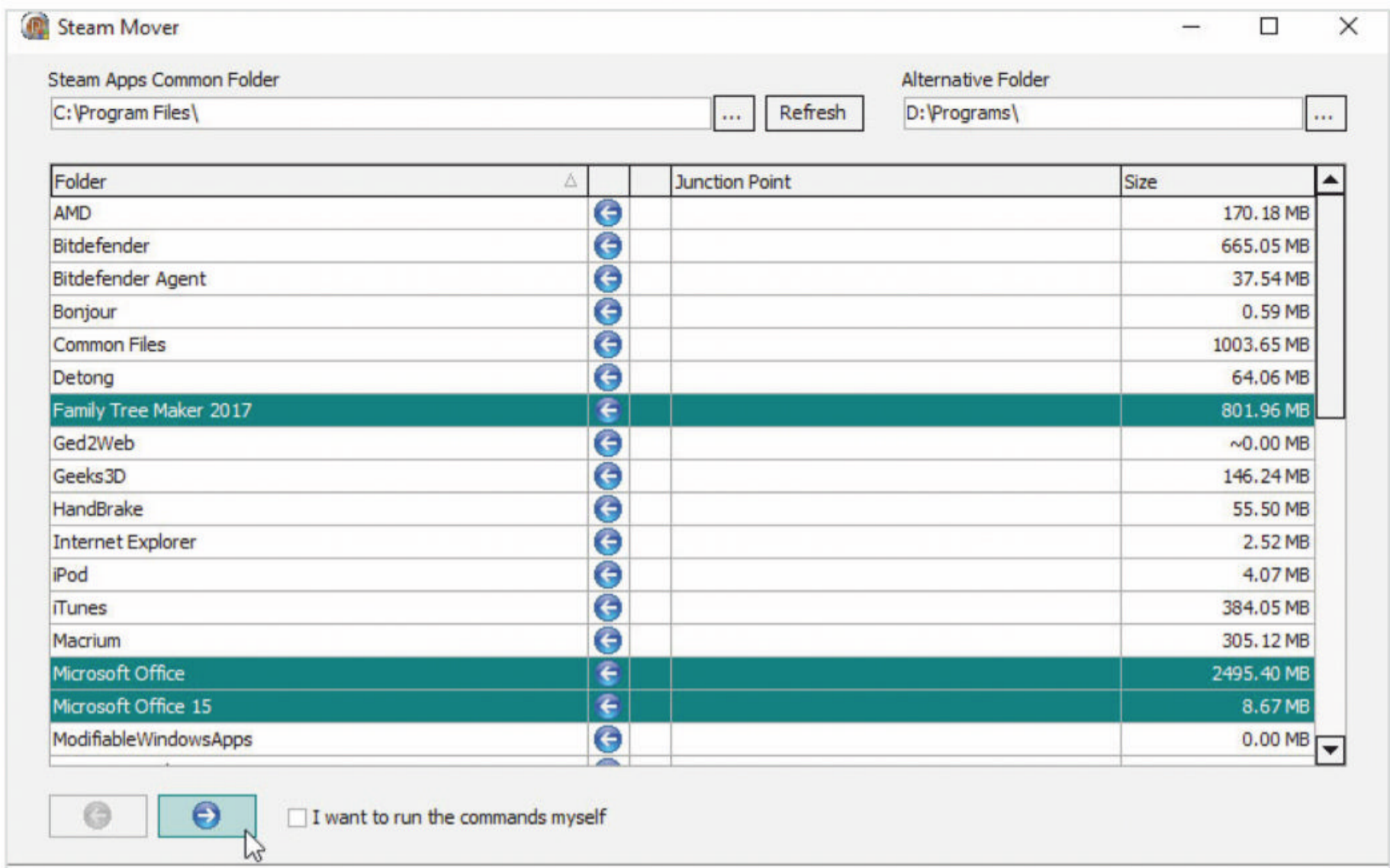
SteamMover enables you to move any program to another drive without reinstalling it.

from the "Program Files" folder to your new drive. One option might be to uninstall and reinstall, but that comes at a cost of losing your preferences, and assumes the program in question allows you to choose where to reinstall the program.

A simpler, foolproof option is to use SteamMover (**www.traynier.com/ software/steammover**). This clever tool moves your program files to your data drive, but leaves a "symbolic link" in its place. This shortcut fools Windows into thinking the programs are still on your C drive, so they continue to work seamlessly. It's easy to use: Click "…" under "Steam Apps Common Folder," and select "C:\Program Files." Ctrl–click the programs you plan to move, based on their size and how frequently you use them, then click the right arrow button to move them all across. Changed your mind? Simply select your program and click the left arrow button to move it back, no questions asked. Windows 64–bit users should also check the "C:\Program Files(x86)" folder for 32–bit apps to move.

## Move data to a new drive
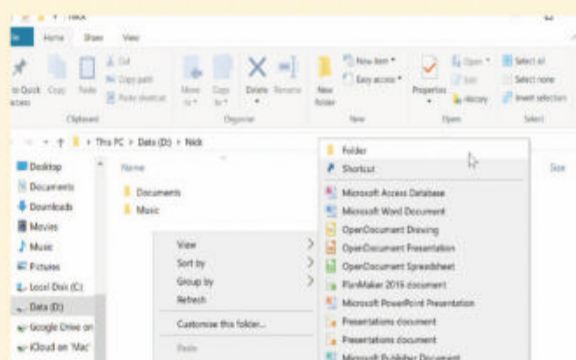






**1** SET UP NEW FOLDERS Open File Explorer and browse to your new drive. Create a new folder named after your username. Inside this, create more folders to match those shown under "Folders" in File Explorer's "This PC" view: "Documents," "Photos," "Downloads," and so on.
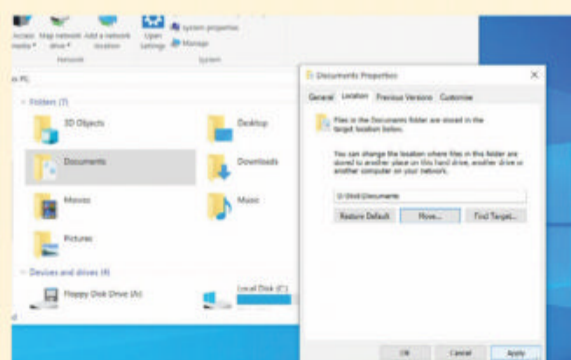
**2** MOVE USER FOLDERS Browse back to "This PC." Right-click "Documents" and choose "Properties > Location tab." Click "Move…" to browse to and select the "Documents" folder you just created. Click "Select Folder" followed by "Apply." When prompted, click "Yes" to move your files and folders to your new drive.
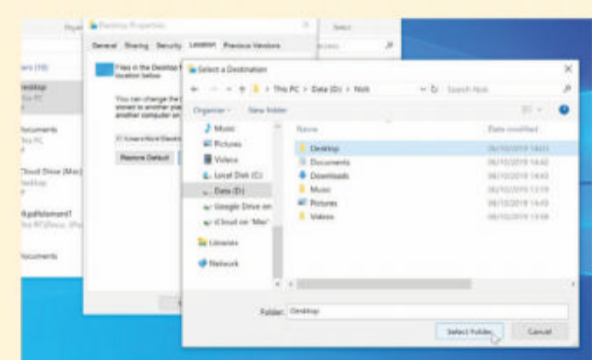
**3** RINSE, REPEAT Now repeat the process for all the other folders listed – be prepared for a long wait if you have large folders to move across to your new drive. The benefit of this approach is that once complete, you'll have freed up space on your system drive without having to delete anything.

# Upgrade your hard drive

Another way to increase storage is to migrate Windows to a separate, faster SSD drive.

Why not turn your problem of storage space – or lack of it – into an opportunity? If you've not done so already, now is the perfect time to investigate one of the most effective upgrades money can buy: a fast solid-state hard drive to run Windows and your programs on. Switching from a clunky old hard drive to an SSD is like leaving the Stone Age. Windows loads in under a minute, apps open in a matter of seconds, and your computing life is no longer held up by clicking and waiting for files to load.

With SSD prices tumbling to put even relatively large amounts of storage space in your hands for a modest sum, there's never been a better time to make the move. The upside? Your old drive can stay in use as a dedicated drive for data, with tens – if not hundreds – of gigabytes of space freed up by moving Windows and your programs across to the new drive.

It's a three-step process: First, work out what your PC can accommodate, and pick the appropriate drive for the task. Once done, investigate the practicalities of fitting it to your PC, and then finally follow a method for migrating everything (or the key elements) off your old drive and on to the new one.

## Choose the right drive

If you're a laptop user, you're basically looking for a larger single drive to accommodate Windows, applications, and a decent amount of personal data.

This may involve moving from a relatively small SSD drive (say 128GB or less), or migrating from a large (say 1TB or bigger), but cumbersome drive. As always, while it's tempting to save money in the short term, try to stretch your budget to future-proof your purchase for as long as possible. With 500GB SSD drives weighing in at under $, this should really be your minimum spec. Increase your budget to $120, and you'll find several 1TB SSD drives falling within your grasp, too. You'll then need to invest in a USB or NAS drive for those files you access less frequently.

If you're looking to upgrade a desktop PC, check to see whether your case can accommodate a second drive in addition to your current one. Chances are it can, giving you get the best of both worlds: a new SSD drive that can be smaller (say 256GB, or 500GB for those with a gaming habit or the need to run virtual machines), plus your old drive now exclusively used for data storage.

If you have a modern PC with support for the M2 NVMe interface (a small slot on the board into which SSD drives shaped like RAM sticks are plugged), pay the small premium for this type of SSD storage, because it's up to six times

faster than SSD, never mind regular hard drives. Samsung's 970 EVO Plus is currently the best – 250GB will set you back around $130, and 500GB around $175.

## Fit the drive

The walkthrough opposite reveals how to clone a drive using Macrium Reflect Free. Note: Both old and new drives need to be connected to your PC at the same time. For desktop users, this means screwing in your new drive to an available 2.5-inch or 3.5-inch bay if connected via SATA, or slotting it into the NVMe slot, before pushing it down and holding it horizontally in place using the screw supplied.

Laptop users have a choice: If you plan to keep the old drive as additional storage, invest $15–20 in a cheap USB 3.0 2.5-inch enclosure, and fit the new drive in there. If not, purchase a USB-to-SATA adapter from eBay for as little as $6, and use that to temporarily connect your new drive to a spare USB port. Once the old drive has been cloned to the new one, swap the two around, and your laptop should boot with all settings and data intact.

> " *With 500GB SSD drives weighing in at under $120, this should really be your minimum spec.*



This $10 adapter makes it easy to attach any bare drive to your PC or laptop's USB port.



Watch Windows 10 (and startup apps) load in under 30 seconds with NVMe storage like this Samsung.
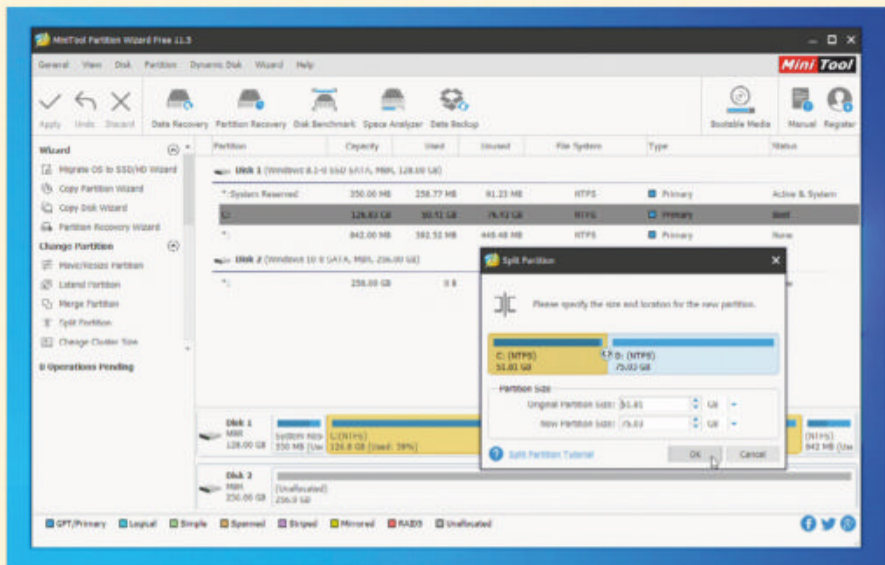
**1** PARTITION OLD DRIVE Desktop users planning to migrate Windows and apps to an SSD while leaving data behind should first use MiniTool Partition Wizard Free (**www.partitionwizard. com**): Choose "Split Partition" and drag the slider as far left as it can go. Click "OK" followed by "Apply." Reboot when prompted.
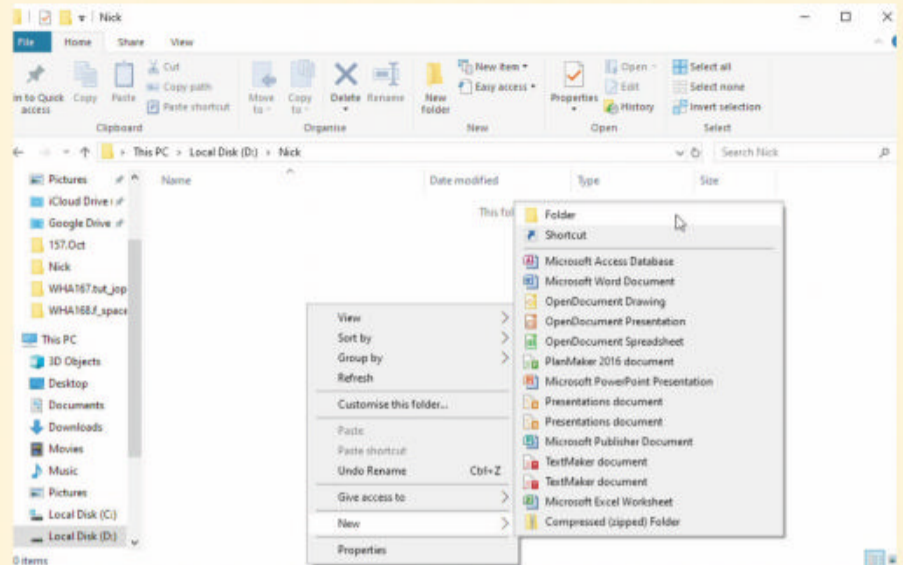


**2** MOVE DATA TO NEW PARTITION Once complete, you should follow the three-step guide on the previous page on moving data to your new drive, using your newly created partition as the target. Download and install Macrium Reflect Free from **www. macrium.com/reflectfree.aspx** if you have not already done so.
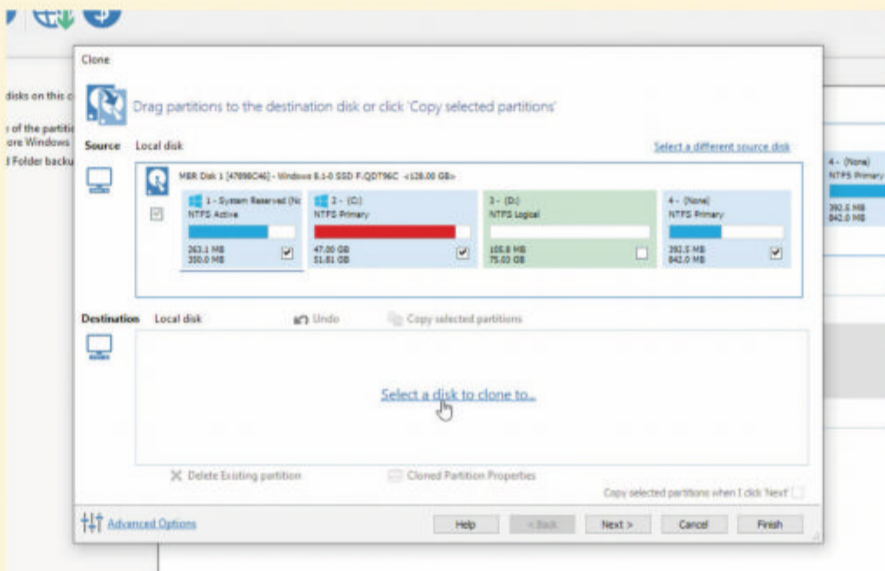


**3** SELECT PARTITIONS TO CLONE Launch Macrium. Select your Windows drive and click "Clone this disk." Make sure only the partitions you need will be copied across: System Reserved, the Windows partition, and any hidden partitions at the end of the drive. Uncheck any others, then click "Select a disk to clone to."
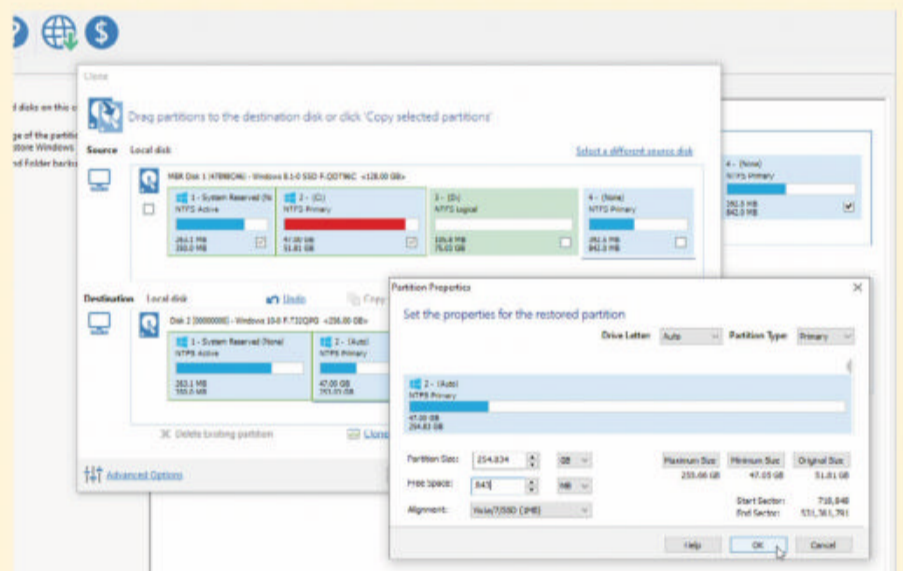


**4** SET TARGET DISK Select your new SSD drive – the one with no partitions assigned. Drag each partition across – you need to click "Cloned Partition Properties" to resize your main partition after dragging it across. Set "Free Space" to match the last partition's size, click "OK," and drag the final partition over.
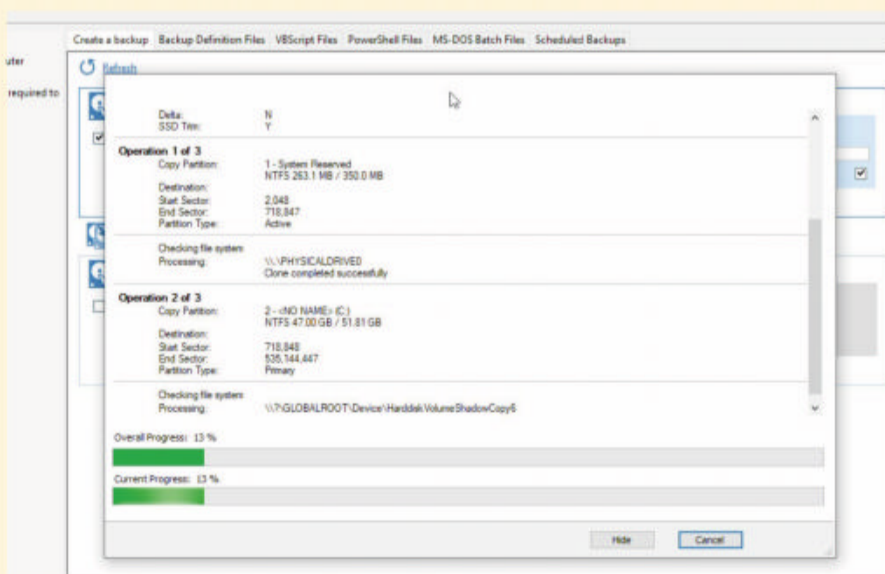


**5** WAIT AS DRIVE IS CLONED Click "Finish." Uncheck "Save backup and schedules as an XML Backup Definition File" and click "OK" to perform the cloning operation. Each partition is copied in turn, a quick file check is done, then the actual cloning process takes place. Be patient – this may take some time.



**6** FIT NEW SSD DRIVE Shut down your PC. Laptop users should swap out the current hard drive for their new SSD drive; desktop users need to reboot and make sure the new SSD drive is the primary boot device in the UEFI/BIOS settings. If all is well, Windows should boot – and much quicker than before. **TL**

# HELP STATION

Expert solutions for everday problems.

*If your laptop drive fails, replace it with an affordable external drive.*

### SECURITY
## Malwarebytes vs Firefox prefs file

Every time Malwarebytes 4.0 runs a scan on my PC it flags my Firefox prefs.js file as containing a PUP.Optional.Conduit. I presume this is linked to some add-on, but how can I find out which? And should I remove it?
Jonathan Glassier

PUP.Optional.Conduit refers to an online platform used to create custom toolbars and apps. It's known to change browser settings and display potentially dangerous adverts. However, it's not actually malware, so don't panic. Start by making sure that Firefox is closed before instructing Malwarebytes to quarantine the file – this will ensure the file is actually removed. Firefox will then recreate a new prefs.js file. If the file keeps getting flagged, you'll need to browse to your Firefox profile folder (press Win-R, type %appdata%\Mozilla\Firefox\ Profiles\ and hit [Enter], then double-click the folder ending in '.default'). Right-click prefs.js and choose Edit to open it in
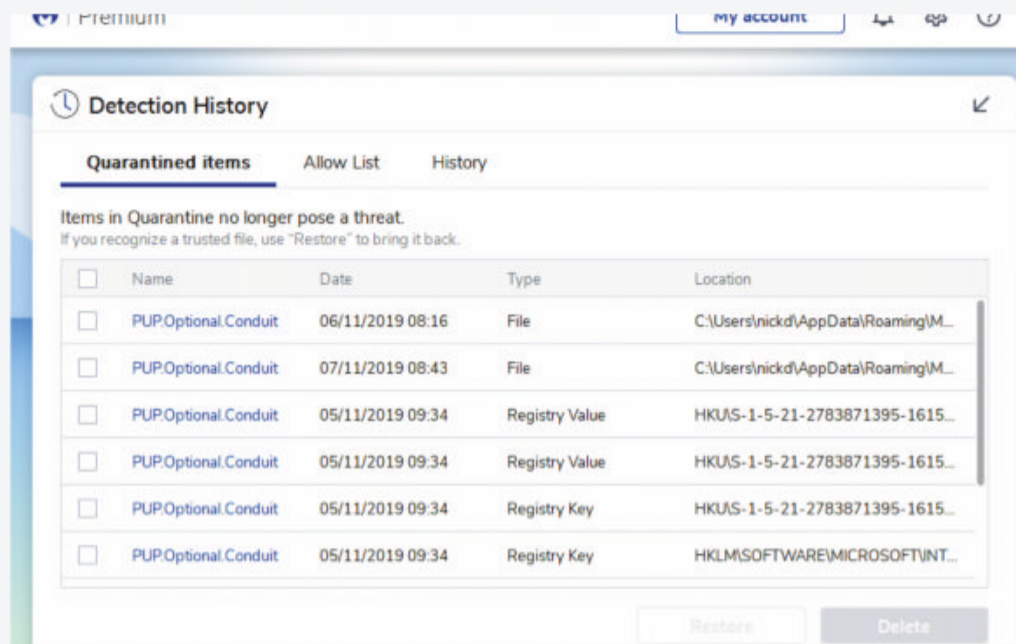


Malwarebytes can't properly quarantine prefs.js if Firefox is open.

Notepad to see if you can easily locate any suspicious-looking entries. If you can link them to a specific add-on (including any search engines you may have added), try removing it to see if that removes the entry and resolves the problem – do so via about:addons (for extensions) and Options > Search (for search engines). If you can't find the culprit, but you're happy with your current setup, then PUP. Optional.Conduit is more an irritation than a genuine threat, so consider just ignoring it.
Carrie Marshall

### HARDWARE
## CDs and DVDs are not detected

For the past two months I've been unable to use CDs or DVDs in my laptop. I've tried different apps, but I always get the same error message: "Please insert a CD". I'm running the latest version of the Windows 10 Insider Preview.
Walter Tuchschmid

Sadly, this could well be hardware failure. Start by eliminating all other possible causes if you haven't already: run through the steps at **https://support. microsoft.com/kb/314060/** to verify it's not a driver or Windows-related issue.

You could even go as far as to take a drive image of your current setup, then reinstall a retail copy of Windows 10 from scratch to see if the problem is resolved; either way, you can then roll back to your current Insider installation.

If hardware failure is confirmed, then you have a choice: first, source a replacement drive for your specific laptop model – you may need to search eBay, and track down your laptop's service manual online for the procedure to follow to replace an internal drive.

If this sounds like too much

hassle, then an external replacement drive is an affordable alternative: around $20–30 on eBay or Amazon.

Note, however, that you may need two spare USB ports, one of which will supply power to the drive.

Ian Sleightholm

## SECURITY
## Have I been compromised?
I received an email that concerns me. The subject line appears to list a password that contains some of the characters in the correct order that I've used, and then the email body is basically trying to extort money from me, claiming that I've visited an adult website and that my webcam recorded me 'having fun'. I'm being asked to pay $2,000 to avoid embarrassment.

Given I've never visited this (or any adult site), I'm pretty sure it's a scam, but those password characters worry me.
David Hargeaves

The email is a complete scam, but there's some truth behind it. First, you've been targeted because your email and some old passwords exist on a database containing leaked passwords and emails. The threat itself is empty, but it's a timely reminder to make sure you regularly update your passwords and avoid reusing the same ones. Use a free tool like LastPass (**www.lastpass.com**) to generate strong, random and unique passwords for your online accounts, and make the effort to update them every six months or so. Also consider employing two-factor authentication (2FA) for particularly sensitive accounts – use Authy (**www.authy.com**) to enable you to supply 2FA codes from more than one device.
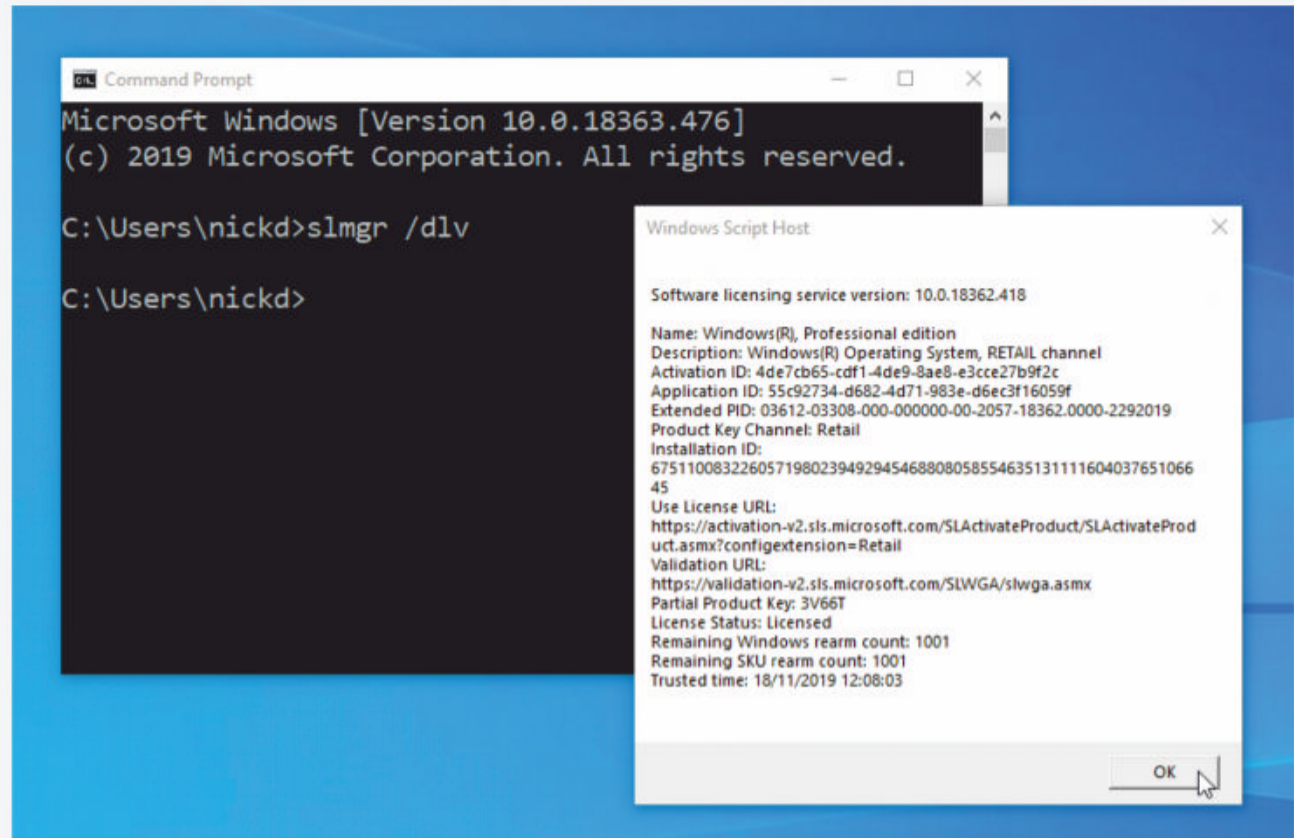


## HARDWARE
## Can my PC support 4K?
I'm wondering if my Intel Core i3-6100 with onboard graphics is capable of running an Ultra HD monitor?
Dafydd Lewis

Most Intel Core processors from 2010 on support 4K displays – for basic usage at least. The Core i3-6100 has onboard Intel HD Graphics 530, which can display 4K images and play certain video formats, but will perform poorly when it comes to games. We contacted Dafydd to find out which motherboard was powering his PC – this is critical because the HDMI output may not support 4K at the recommended refresh rate of 60 Hz. Sure enough, his Asus Z170-A only supported 4K output via HDMI at 24Hz. Its DisplayPort connector does, however, support 60Hz, which means he needs to source a 4K monitor with a DisplayPort input to ensure the best possible picture without having to invest in a dedicated graphics card.
Nick Peers

You need a retail licence to move Windows to a new PC.

> *You've been targeted because your email and some old passwords exist on a database containing old leaked passwords and emails. The threat itself is empty, but it's a timely reminder to make sure you regularly update your passwords and avoid reusing the same ones.*

## WINDOWS
## Activate Windows on my new PC
I'm looking to replace my old PC with a self-built model. I took advantage of the free upgrade to Windows 10 from Windows 7, but am trying to determine if I can transfer my Windows installation – a digital license – to this new PC from the old computer. Any help gratefully received.
Anita Rawlinson

There's a common misconception than when you accepted the free upgrade to Windows 10 you automatically tied your copy of Windows to the PC you upgraded on. That's not necessarily true: if your old copy of Windows 7 was a retail one (in other words, not an OEM licence, or pre-installed by your PC manufacturer) then you should be able to transfer it to your new PC. To verify this is the case, open a Command Prompt or Powershell window, then type the following and press [Enter]:
**slmgr /dlv**
After a short pause a pop-up window should appear – if the 'Product Key Channel' is listed as

Retail you should be fine to reactivate it on your new PC. You may need to use the Activation troubleshooter ('Settings > Update & Security > Activation > Troubleshoot') to get things working – make sure you're signed into the same Microsoft Account on your new PC as you used on your old PC.
Ian Sleightholm

## STORAGE
### Rattling dead hard drive
My three year-old external hard drive stopped working when my Mac showed a warning to back it up and reformat. It now makes a rattling sound when turned on and won't mount at all. What can I

Even if your hard drive doesn't work, ensure you break it up as thoroughly as possible before recycling.

Windows Key Finder also works with Microsoft Office.

do to rescue its contents?
John Martin

Sometimes, before a hard drive fails, you get sufficient warning to be able to rescue as much as you can from it before it packs up completely, as it will continue to mount on your Desktop. In your case, it seems to have suffered internal mechanical failure too rapidly to allow that. Avoid powering it up at all until you've decided what to do about this, as that could only make damage worse. Modern data recovery services can dismantle even badly failed hard drives in clean room facilities and mount their platters in special enclosures to recover

data. However, this is very expensive and only likely to be worth your while if the files you have lost are very valuable. Typical costs are thousands of dollars, and there's a limited range of models which are suitable for such treatment. If you can't justify that cost, send the old hard drive for recycling. Before parting with it, even though it isn't working, break it open using a heavy hammer to ensure that no one else could try reading its contents.
Howard Oakley

## MAC
### Out of date firmware
I replaced the internal Fusion Drive in my iMac with an SSD. It has now fallen behind with firmware updates. How can I bring it up to date?
Ian Jamieson

Some years ago, Apple stopped supplying Mac firmware updates separately, and now delivers them inside macOS upgrades, updates, and security updates instead. For example, the macOS Mojave 10.14.1 update, High Sierra Security Update 2018-002 and Sierra Security Update 2018-005 all brought a set of firmware updates which also changed the numbering system for the firmware. Some Macs don't appear to install these correctly, though, and one common feature to such problems is that the internal storage of that Mac has been replaced, normally with a non-Apple product, such as an original hard drive which has been upgraded to an SSD. One workaround is to replace the original storage in order to perform the update, but as 'firmware' is largely stored on disk that may not have any effect when the new storage is swapped back in. That also doesn't help if the original drive has failed, or been repurposed. Sometimes installing macOS from scratch as a clean install onto a freshly formatted disk can address this.

**File Converter** screenshot showing the Template Editor and Field Selector dialogs.
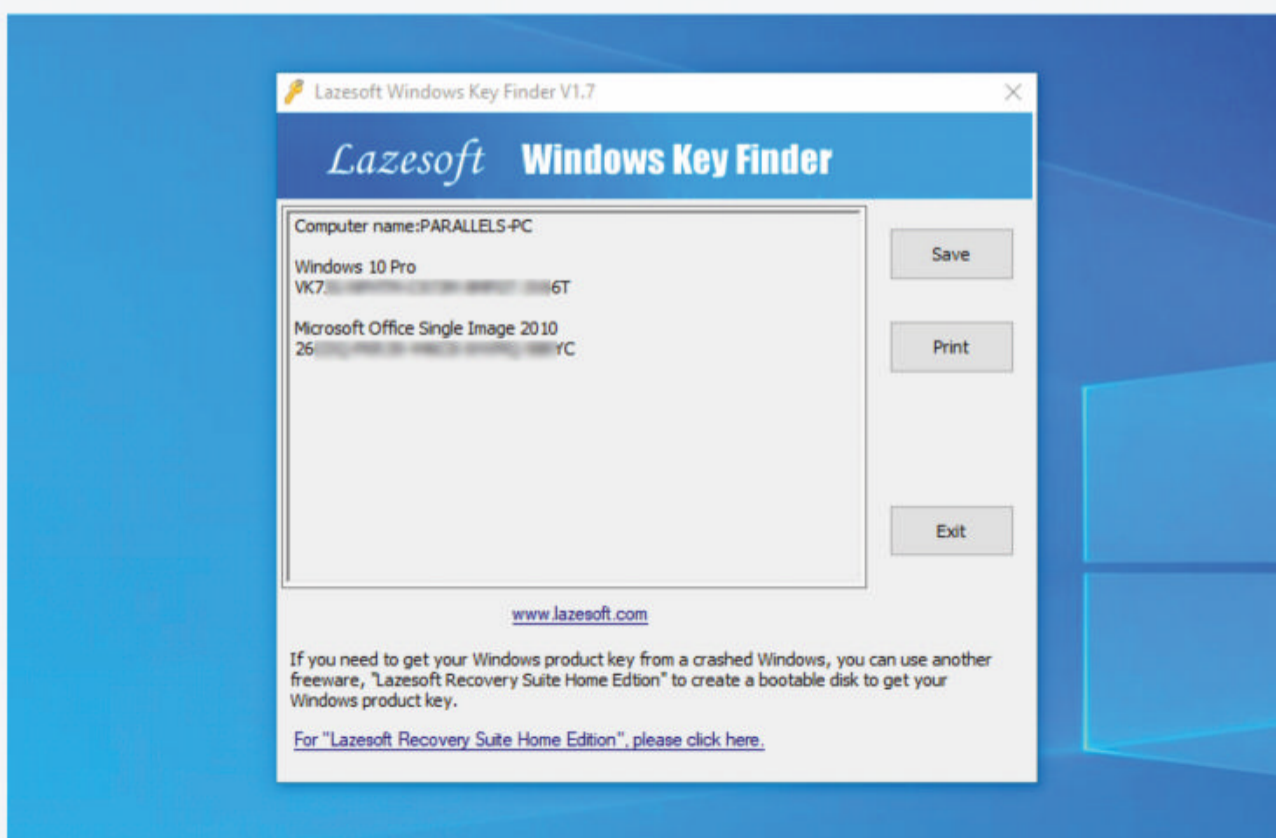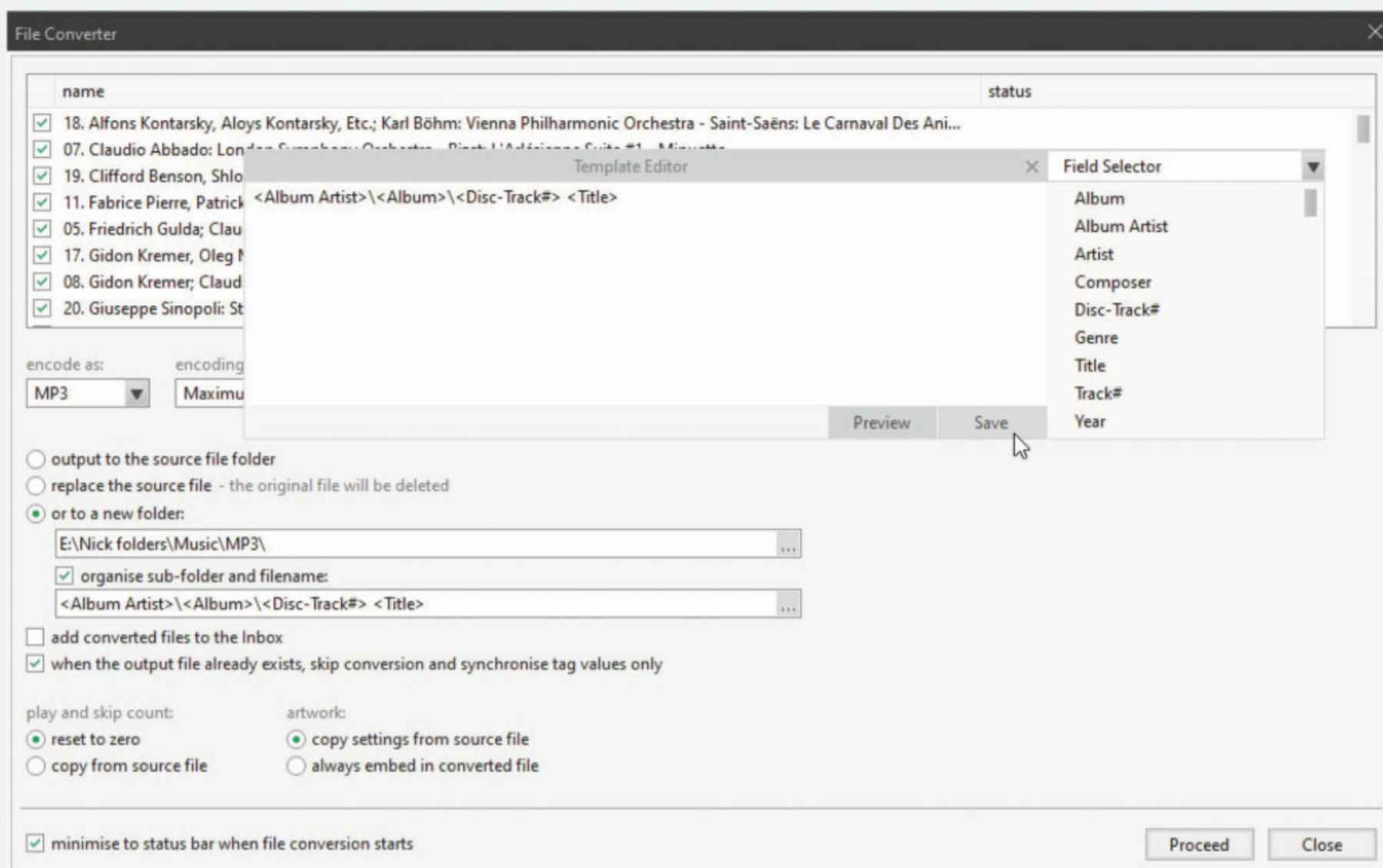
In a few instances, the boot drive doesn't get properly formatted in the first place and may lack the Recovery or other partitions. Sorting these problems out gets very technical, and is probably best done by your nearest Apple store.

Howard Oakley

## OFFICE
### Upgrade needed?

I'm currently running Windows 7 and Office 2010. I really don't fancy paying a monthly subscription for Office 365, so my question is: will I be able to continue running Office 2010 when I upgrade to Windows 10?

Stephan Buser

The good news is that Office 2010 is the oldest version of Microsoft Office that's officially compatible with Windows 10 (Office 2007 should still run but is unsupported). If you're upgrading your current installation from Windows 7 to 10 then the program should be left in place when you update. If you're moving to a new PC, then we recommend uninstalling Office 2010 from your old PC before you install it on your new computer. Make sure you have your product key handy – if you've mislaid it, use Lazesoft Windows Key Finder (**www.lazesoft.com/lazesoft-windows-key-finder.html**) before removing the software from your old PC to reveal it. It's a simple tool, no installation required. Alternatively, you can buy Office Home & Business 2019 online, getting yourself an upgrade without the 365 subscription.

Catherine Ellis

## MEDIA
### Bulk convert audio files

I've been sent some music files in FLAC format. I'd like to convert these to MP3 if possible. What do you recommend?

Paula Redhill

Our go-to music management app (MusicBee – get it from **https://getmusicbee.com**) is the perfect tool for the job. Here's what you need to do to set it up to convert from FLAC (or just about any supported source format) to MP3.

Output your converted files to a new folder to help organise and avoid confusion.

> **"**
> *The good news is that Office 2010 is the oldest version of Microsoft Office that's officially compatible with Windows 10 (Office 2007 should still run but is unsupported).*

Open MusicBee and click the + button to open the file explorer pane on the left. Expand Computer and browse to the parent folder containing all your FLAC files. Once selected, all files within should be displayed in the main pane.

Click the word 'MusicBee' at the top to reveal its menu, then select Tools > Convert Format to open the file conversion tool. Verify all your files are in the top pane. Click the Encode as: dropdown to select your target file type.

You can output the copies to the same folders as the original, replace them or – our choice – select 'to a new folder', ticking 'organise sub-folder and filename' to ensure they remain organised and named correctly.

Tick 'minimise to status bar when file conversion starts' and click Proceed. The window will close, but you can monitor the file conversion progress from the main window's status bar. Once complete, check your files.

# Capture with Snip & Sketch

Whether it's sharing stuff from social media or showing how to use an app, snipping is simple.

**SKILL LEVEL**
Anyone can do it
Straightforward
Tricky in parts

**SUITABLE FOR...**
Windows 10
Windows 8.1
Windows 7

**CARRIE'S BEST TIP!**
You can take a screenshot without Snip & Sketch by pressing the Print Screen (PrtScn) button.

Until very recently, two very useful Windows tools came as separate apps: the Snipping Tool, for taking screenshots, and the Screen Sketch tool, which was part of the Windows Ink Workspace and enabled you to scribble on screenshots. Now they've been combined in the cunningly named Snip & Sketch app, which both snips and sketches. It also shares, either locally via Bluetooth or via mail or messaging apps.

Screenshots aren't just useful for tutorials like this one. You can use Snip & Sketch to grab and annotate part of a web page, and the cropping tool means you can get rid of anything that isn't important. Just remember that if you plan to use your screenshot in any kind of publication, it shouldn't infringe anybody's copyright. Reusing a screenshot of a copyrighted image could land you in hot water.
CARRIE MARSHALL

**UNDO AND REDO**
Particularly useful when annotating or highlighting bits of an image, when accidents often happen.

**NEW SNIP**
Choose to snip immediately or after a few seconds. You then choose what to snip: fullscreen or a selection.

**SNIPPED IMAGE**
Your image appears here, with your sketching overlaid on top. We've used the red pen tool to circle a problem.
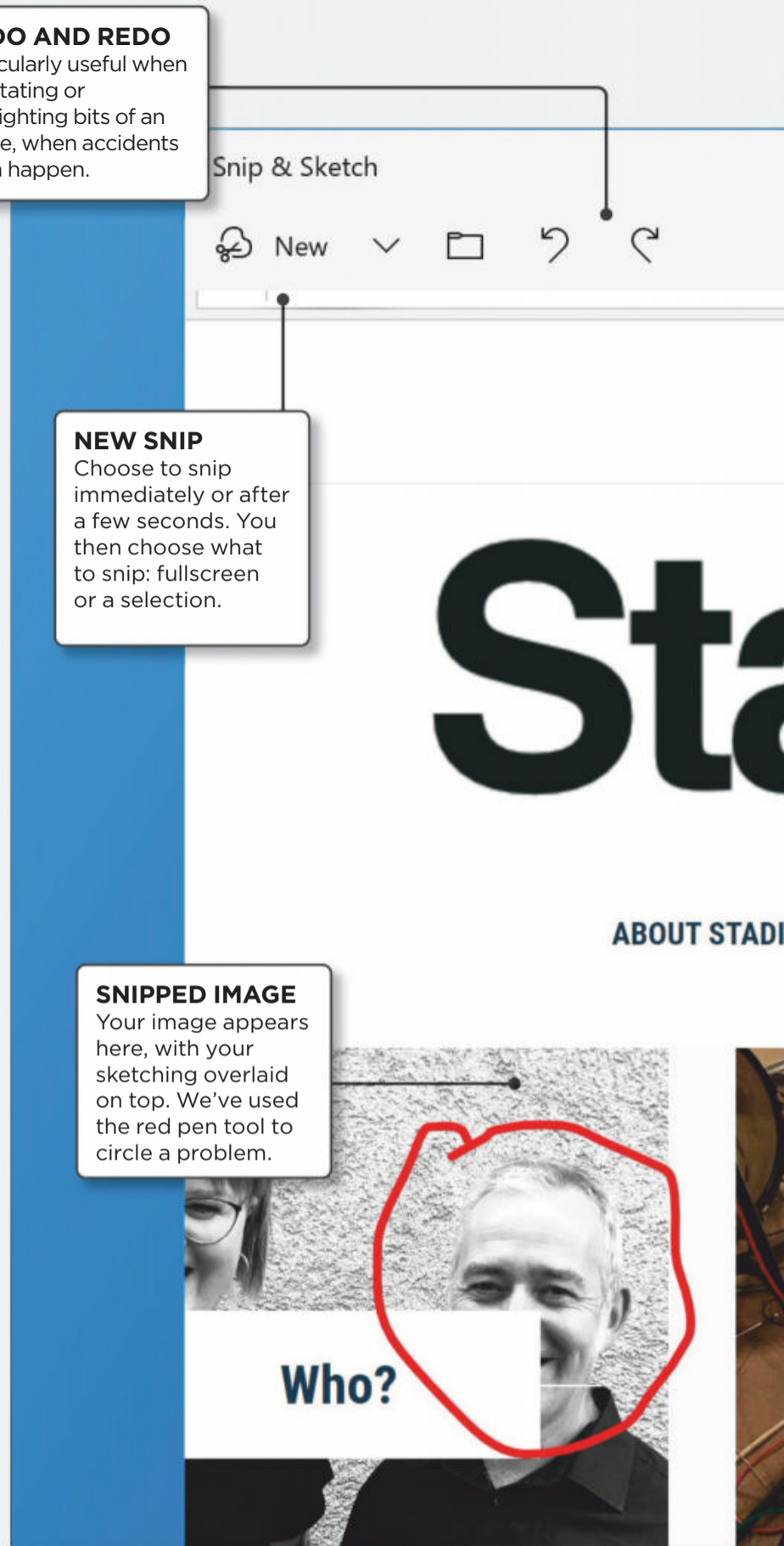
## HOW TO Take and scribble on screenshots
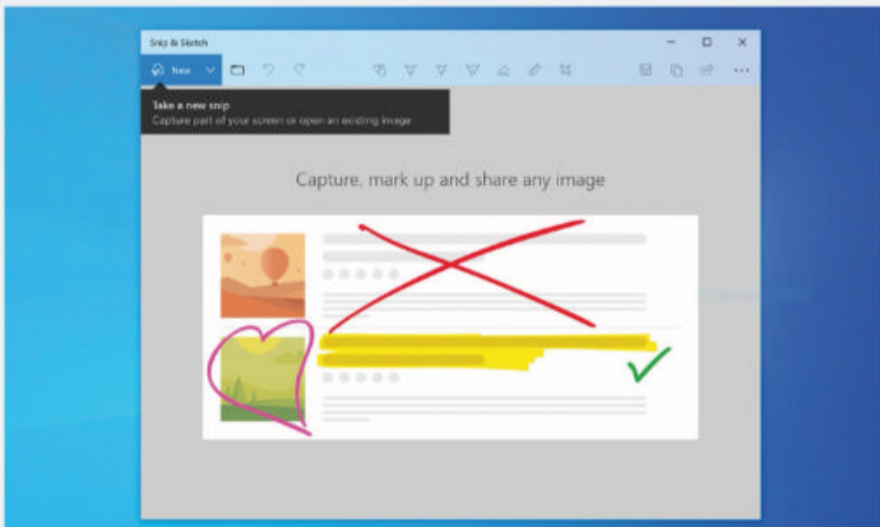
**1** START SNIPPING When you launch Snip & Sketch for the first time you'll see this helpful intro screen, with the New button highlighted and annotated with a tooltip. Unless you want to take a picture of your desktop, the first thing you'll need to do is have something ready to snip open in the appropriate app: the whole point of the Snip & Sketch tool is that it captures what's on the screen of your PC.
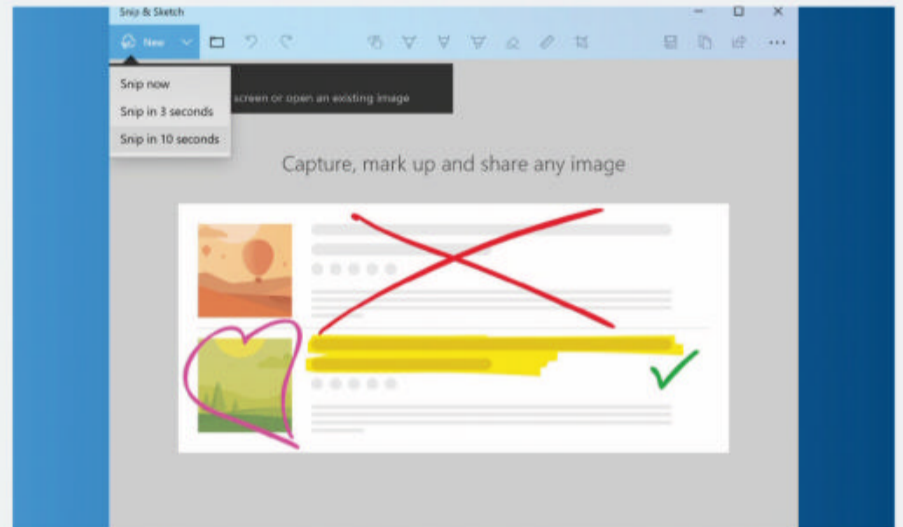
**2** CHOOSE YOUR FORMAT Clicking on New Snip doesn't immediately take a screenshot. First you need to decide whether to take a picture immediately or to wait three or 10 seconds. This delay is useful if you want to take a picture of something fleeting, such as an app's pop-up menu. Once you've chosen whether to have a delay, Snip & Sketch will disappear so you can see your screen.
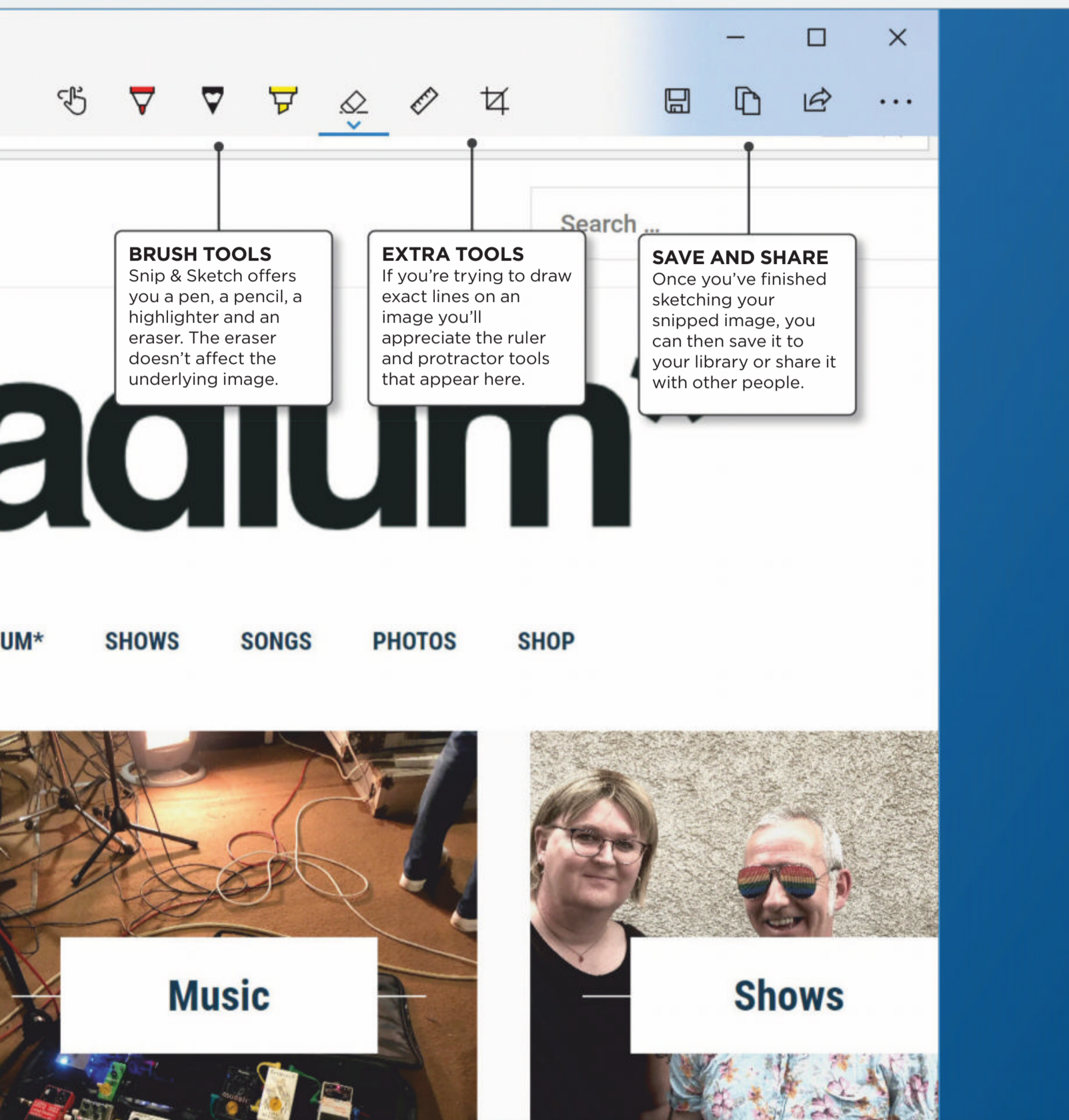
**BRUSH TOOLS**
Snip & Sketch offers you a pen, a pencil, a highlighter and an eraser. The eraser doesn't affect the underlying image.

**EXTRA TOOLS**
If you're trying to draw exact lines on an image you'll appreciate the ruler and protractor tools that appear here.

**SAVE AND SHARE**
Once you've finished sketching your snipped image, you can then save it to your library or share it with other people.

aɑlum

UM*    SHOWS    SONGS    PHOTOS    SHOP

**Music**

**Shows**
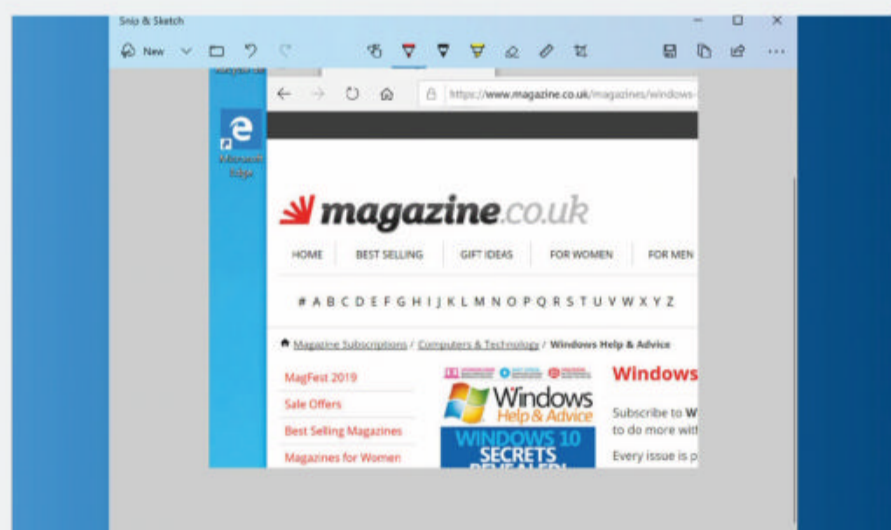
**3** CHOOSE YOUR AREA When Snip & Sketch is waiting to take a screenshot, the screen darkens. You'll see a little toolbar at the top of the screen, from where you select the image you want: a fullscreen image of the entire display, a rectangular snip or a freeform snip. The second and third options get you to draw around the area you'd like to snip. Once you've done that, you'll see the snipped image.
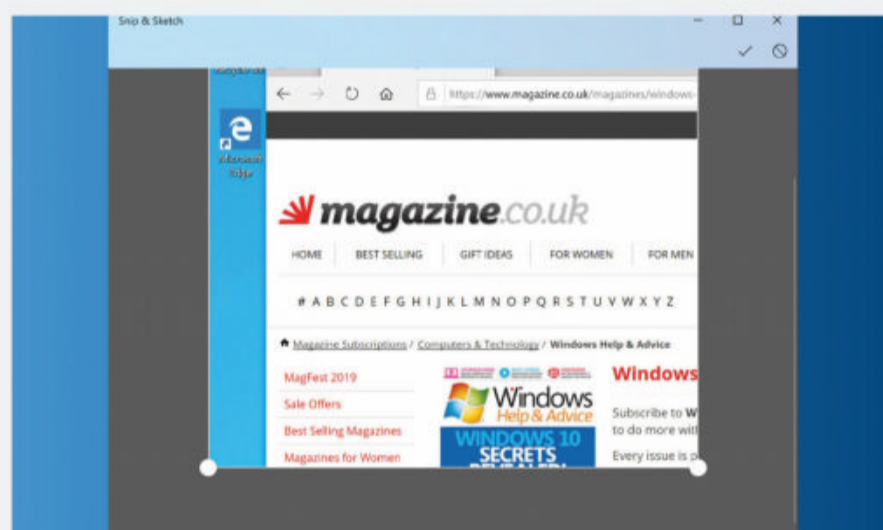
**4** GET THE EDGE If you haven't taken a fullscreen snip, you'll often find that the snipped image isn't quite right: in our image here we've accidentally included a bit of the desktop. No problem. Look at the middle of the toolbar and you'll see some brushes; look to the right of that section and you'll see the crop icon, a rectangle with a diagonal line through it. Click the tick when you're happy.
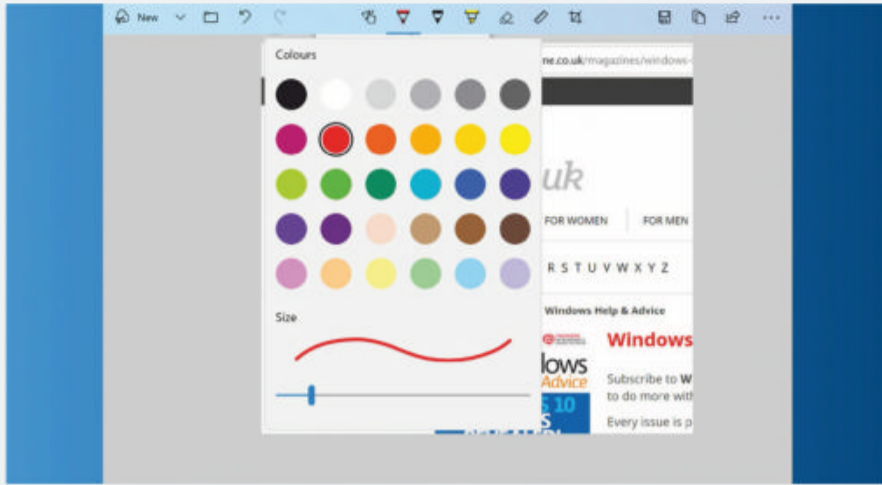
**5** PICK A COLOUR Each of the three brush tools – the pen, the pencil and the highlighter – enable you to choose a colour and nib size. To do that, click and hold the appropriate icon. Here we've brought up the options for the pen brush tool. Click on a colour to select it or use the slider at the bottom to make the tool wider. If you're going to use the tool to handwrite, thin is usually better.



**6** GET SCRIBBLING As you can see from our screenshot, it's easy to highlight or otherwise draw attention to a bit of the screen. If you make a mistake there are two ways to fix it. You can use the undo icon, which is in the toolbar towards the top left of the window, or you can use the eraser tool to the right of the brushes. The eraser removes your drawing, but not the snipped image you drew on.



**7** DRAW PRECISELY Although they're not needed to help us with our quick scribbles, there are two useful tools in the app for anyone who needs to draw with precision: the ruler, shown here, and the protractor, for angles. Press and hold the ruler icon briefly to bring up the choice of ruler or protractor. Tap the icon again to put the ruler or protractor away.
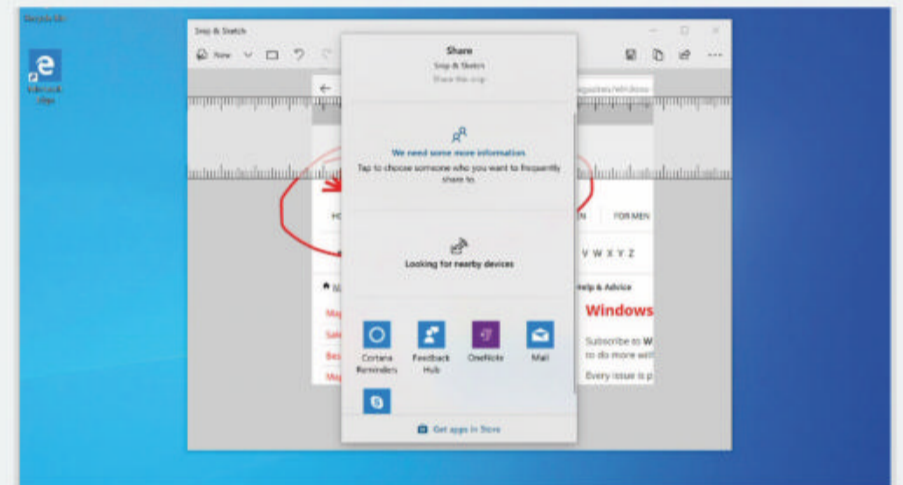


**8** SHARE YOUR SNIP For most of us, snipping is something we do because we want to share the image with somebody else. That might be because someone's said something really silly on social media, or because we thought of a funny caption for something. You can share from within the app by tapping the Share icon, which is the second icon from the right in the toolbar.



**9** SHARE IN A MESSAGE If you've set up a messaging service or email, you can share the snip as a message: the app automatically calls up the relevant service, in this case Windows Mail, and creates a new message with the snipped image already in it. You can then add text and formatting just as you would in any other email, and send it without having to open the Mail app. Just tap on Send.



**10** ADJUST THE SETTINGS If you tap on the More icon – the three dots at the far right of the toolbar – you can tweak Snip & Sketch's settings. For example, you can disable the automatic copying to the Windows clipboard, or you can get the app to automatically add an outline to your snipped images. That one's useful for screenshotting bits of things when planning to use the screenshots in documents. **TL**
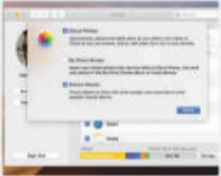
# Manage iCloud Drive

Make the most of Apple's convenient online storage facility.

iCloud Drive is the file storage part of Apple's iCloud services. It's an easy way to access your files from any of your devices, and is similar to Dropbox, Google Drive, and Microsoft OneDrive.

It shows up as a folder in Finder and you can drag files and folders to and from. By default, a copy of everything in your iCloud Drive is stored on your Mac. Files put in iCloud Drive are synced to Apple's server and made available on all Mac and iOS devices on your iCloud account. (Make sure yours are signed in: go to Apple > System Preferences > iCloud on a Mac, and Settings > [your name] > iCloud on iOS.)

Files stored in iCloud Drive are encrypted, both in transit and on the server, as long as you have two-factor authentication enabled for your Apple ID. Confirm this by signing in at **appleid.apple.com** to ensure it's switched on under the Security heading.
KENNY HEMPHILL

## HOW TO Manage iCloud Drive
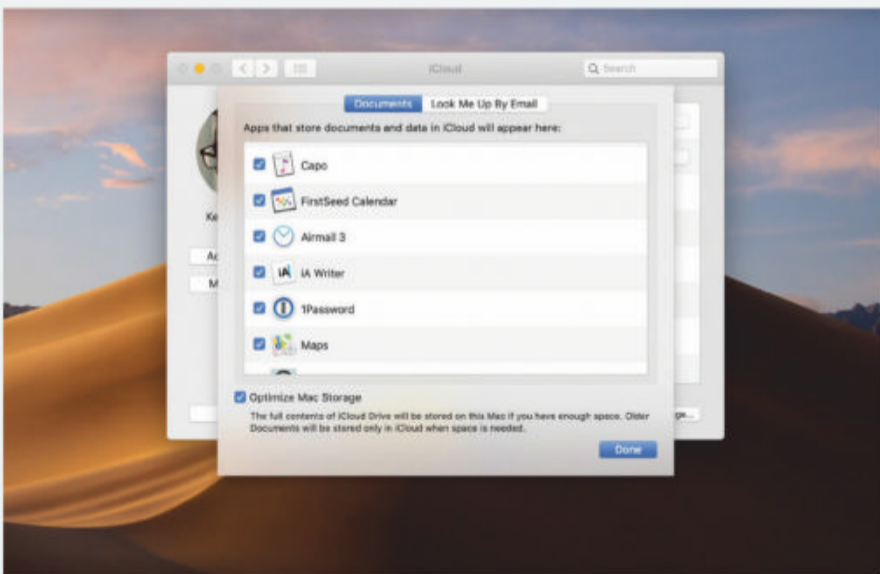




**1** CONFIGURE YOUR MAC APPS In Apple > System Preferences > iCloud, click Options next to iCloud Drive in the list on the right. You'll see a list of apps that store files and other data in iCloud Drive. Clear the box next to apps you don't want data stored for.
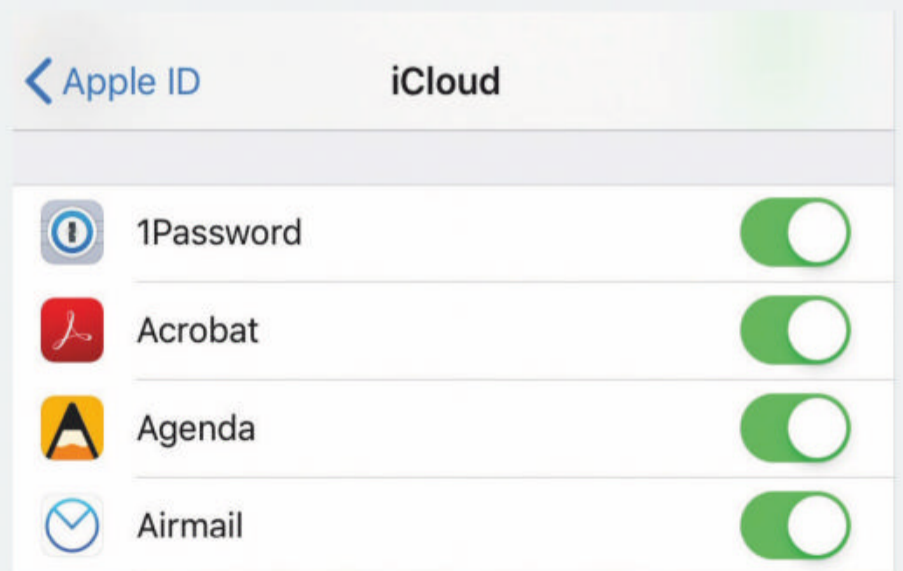
**2** CONFIGURE YOUR IOS APPS On iOS, go to Settings > [your name] > iCloud. Scroll down to the list of installed apps; toggle off any apps you don't want data stored for in iCloud Drive. Note, though, that this might hinder some apps' functionality.
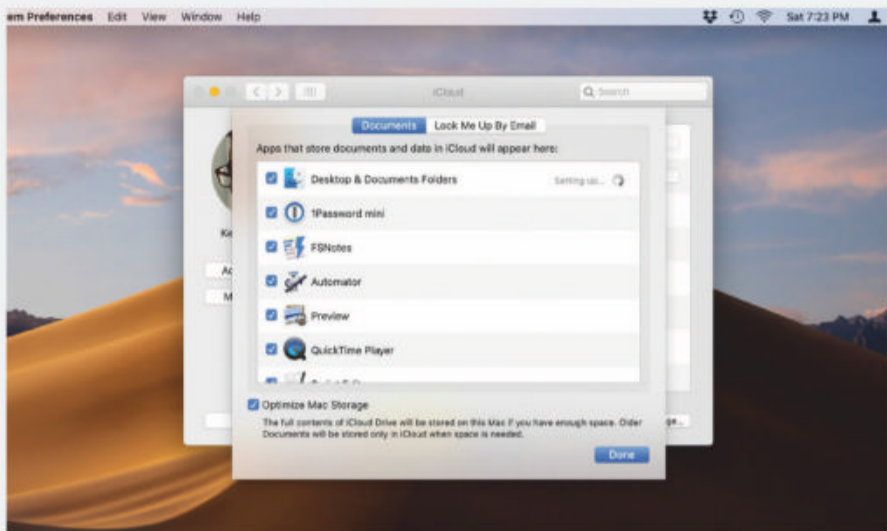
**3** PUT YOUR DESKTOP ONLINE You can have the same Desktop and Documents folders across compatible Macs, and access them from iOS devices and the web too. Click Options next to iCloud Drive, then tick Desktop & Documents Folders.
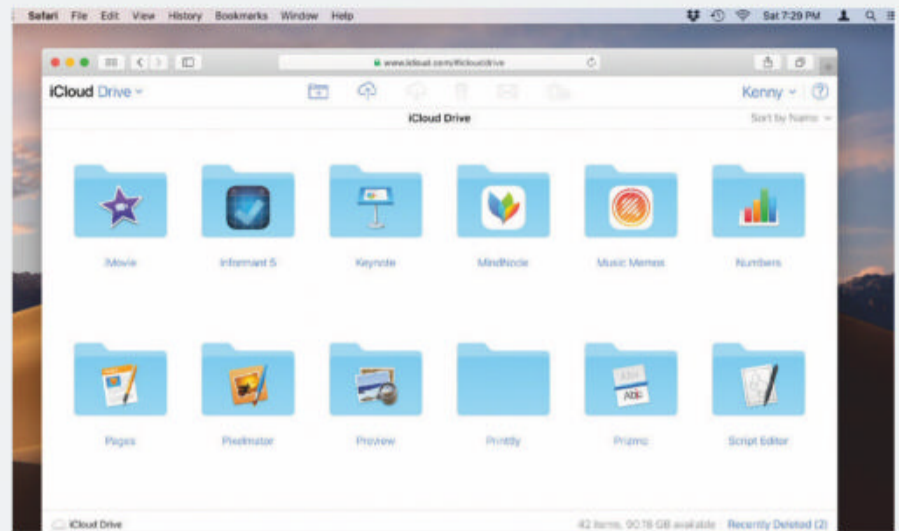


**4** ON THE WEB With those folders set to sync to iCloud, you can sign in at **iCloud.com** in a web browser on other computers. Click iCloud Drive, then open the Desktop or Documents folder to access files saved to those places on your Mac.
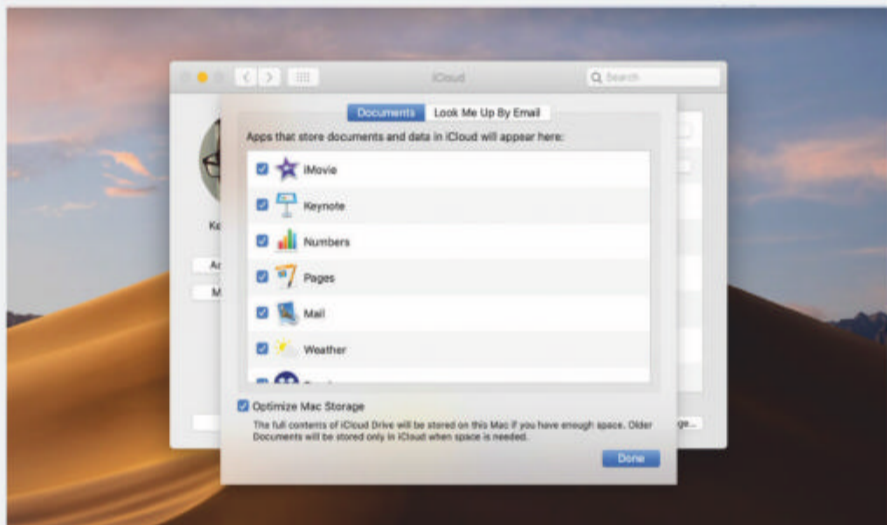


**5** LOW ON LOCAL STORAGE? If your Mac is filling up, iCloud Drive can intelligently free up space: in its options, check Optimise Mac Storage. It will try to keep files locally that it thinks you'll need. Others are redownloadable by clicking their cloud icon.
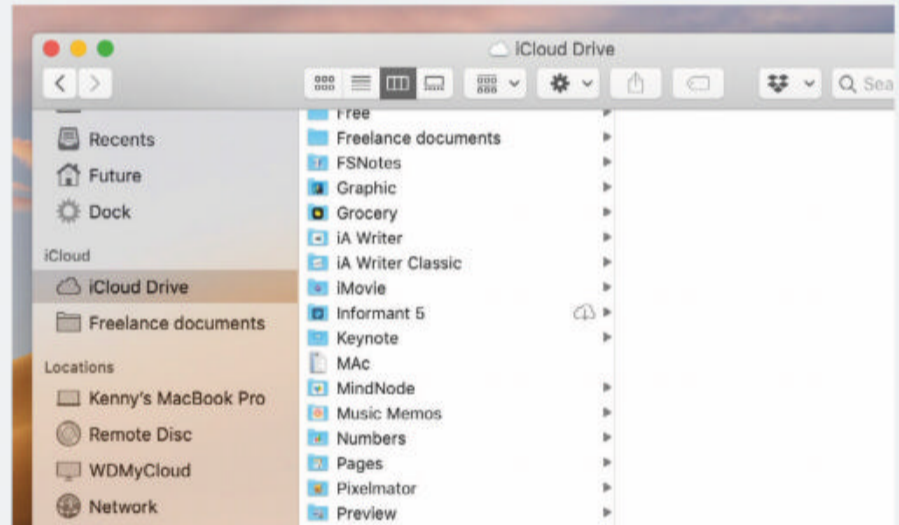


**6** CREATE FINDER SHORTCUTS You don't have to start at the top of iCloud Drive to find something. Just like regular folders on your Mac, you can drag folders from it to Finder's sidebar or the right end of the Dock to create shortcuts.
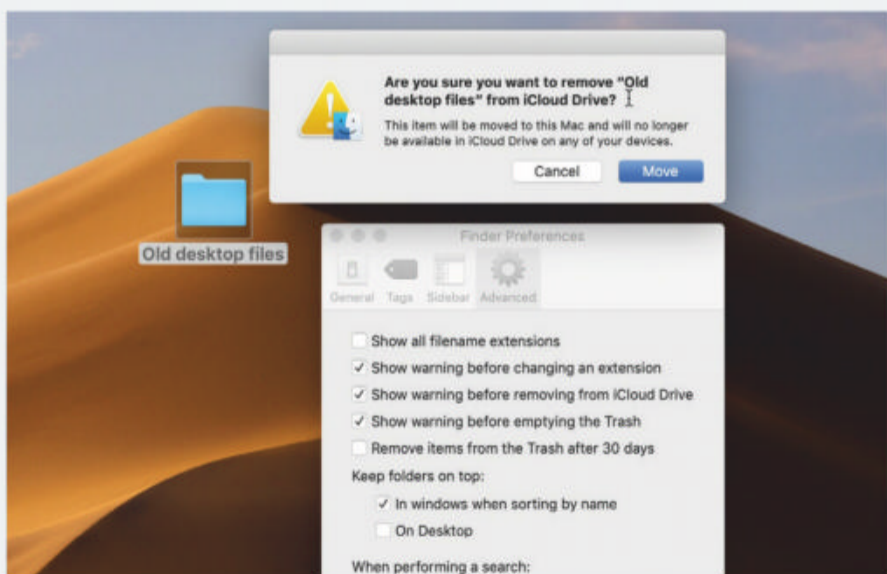


**7** PROMPTS WHEN REMOVING Finder asks for confirmation if you try to move online files to your Mac's local storage. If that gets annoying, go to Finder > Prefs > Advanced and turn off "Show warning before removing from iCloud Drive".
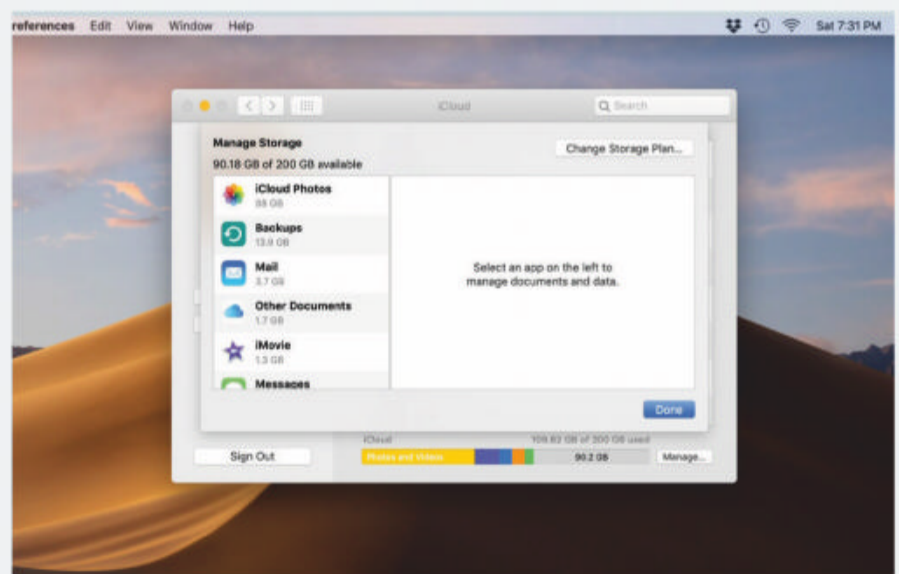


**8** GET MORE SPACE The space available on iCloud Drive is the capacity of your iCloud account minus other data stored in it (see tip, top left). To add more, go to iCloud's prefs, click Manage, then Buy More Storage/ Change Storage Plan. **TL**

# Get creative with Spectre

Unleash your imagination with this easy long-exposure photography app.

**JARGON BUSTER**
Exposure is terminology carried over from traditional DSLRs. The camera's sensor is covered by a shutter that moves to expose the sensor. Long exposures are blurrier, but can be more dramatic.

**GENIUS TIP**
Using a tripod doesn't need loads of extra kit — the GorillaPod GripTight One costs under $40, holds your iPhone securely, and can be mounted to virtually anything.

Apple's default camera app is good, but it could be better. With the hardware on iOS devices becoming ever higher-resolution, and the computational capability of devices themselves on the rise, Apple's simple, point-and-click app means keen photographers generally have to look elsewhere if they want to wrest some control back from devices that are sometimes a little too "helpful".

Luckily, here at Mac|Life, we regularly test and review apps that allow far more control over what your phone does when you press the shutter button.

Spectre Camera ($4.49) is one of our favorite such apps. One of the key benefits of a "proper" camera is the ability to blur motion by using a slow shutter speed. This is complicated: knowing just how long to open the shutter for, and

having the equipment to hold your phone steady, make long-exposure photography a bit of a dark art. Spectre does things differently, shooting hundreds of exposures and averaging them together to produce a finished shot.

The app is really powerful, despite its simple-looking controls, and there are a few useful photographic tips and tricks you can use to produce the attractive results the developer boasts about.

The light trails effect we look at here can be applied just as creatively to things other than just light. When photographing flowing water, for instance, you can achieve a dreamlike quality to your pictures. Read on to master this excellent piece of software.
DAVE STEVENSON

> " *There are a few useful photographic tips and tricks you can use to produce the attractive results the developer boasts about.*

## HOW TO Take long exposures
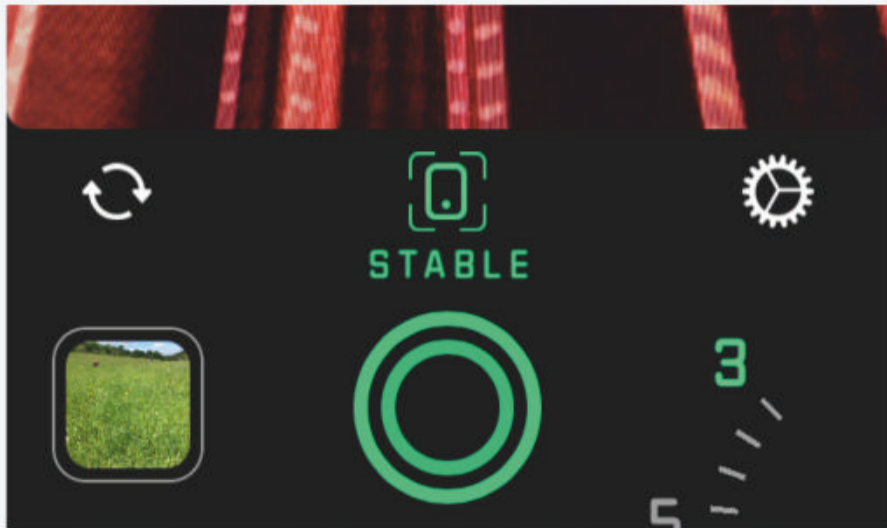


**1** STEADY AS YOU GO Spectre makes much of its ability to shoot long exposures handheld, but take it from us: step one is a tripod or suitable mount (as iPhones don't weigh much). Without one you're definitely not going to get the best photo.
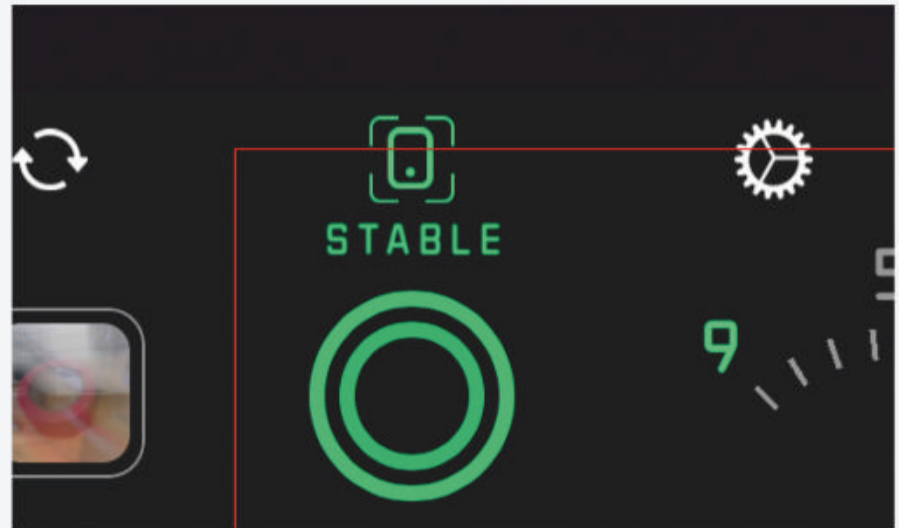


**2** GET THE DURATION RIGHT The dial on the right lets you choose a duration of three, five, or nine seconds for how long the sensor is exposed to light. Use a longer time to exaggerate movement, or for slower-moving subjects, and vice versa.
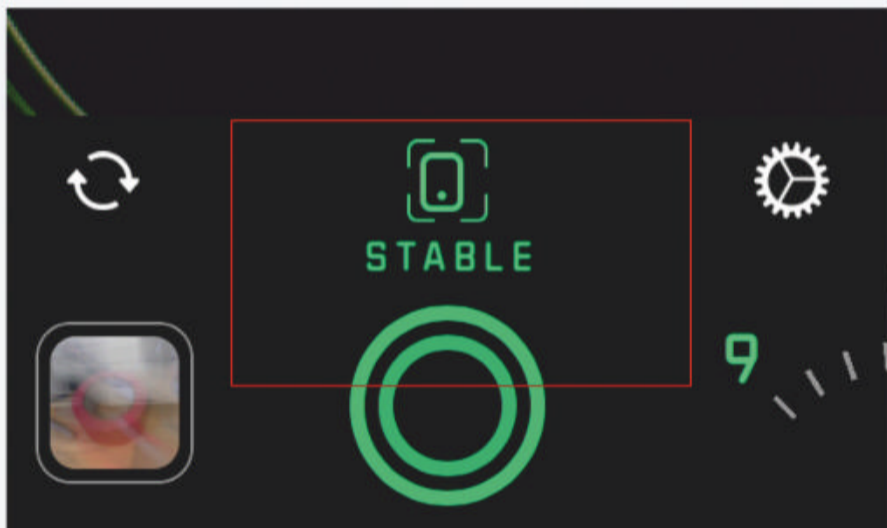


**3** HOW STEADY ARE YOU? The stability indicator is very useful, although it doesn't negate our earlier advice about using a tripod. If Spectre thinks you're holding your phone steady enough to shoot a sharp exposure, it displays a "stable" message.
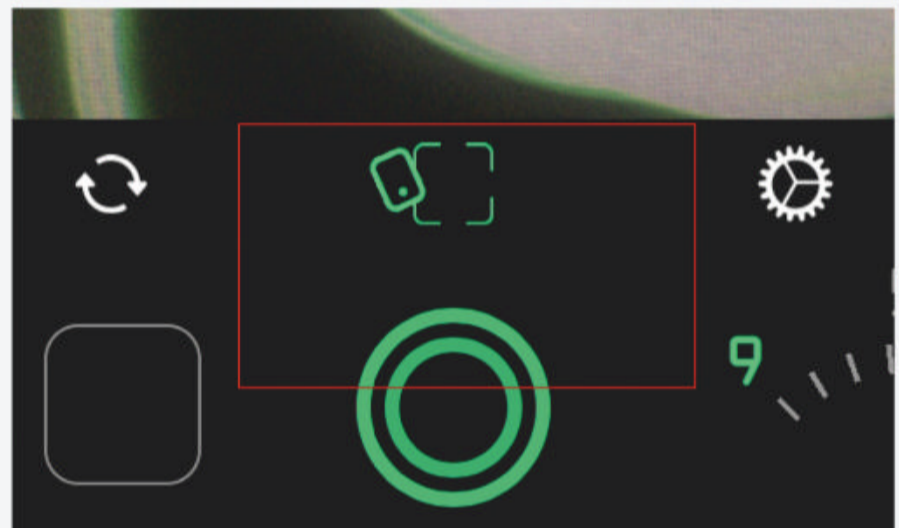


**4** IN COMBINATION Poor results don't just happen when the top-centre icon is like above. It's possible to see the stable indication and still get blurry pics. If shooting hand-held, set a shorter duration by swiping through the options in step two.
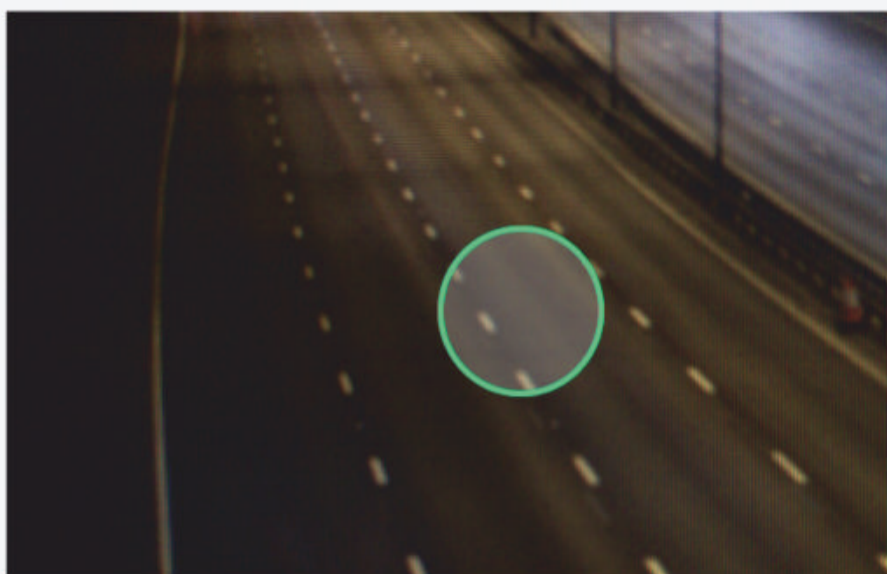


**5** A TRICK OF THE LIGHT If you turn on Light Trails (top-left icon), objects in motion will streak across the frame (think car lights on a motorway). Turn it off and Spectre averages frames together: anything that moves between frames will simply vanish.
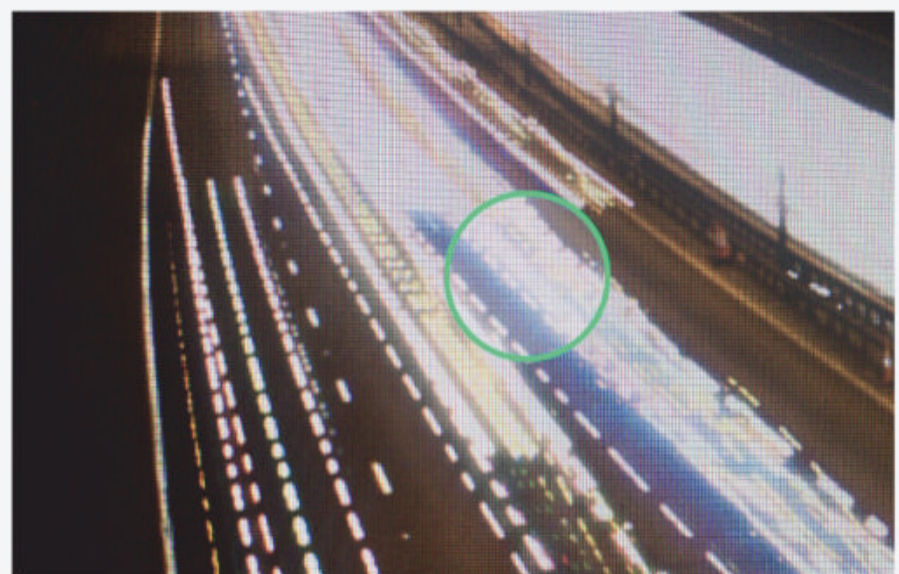


**6** LIVE PREVIEW Spectre shows you the progression of your image while it shoots. If you think your frame looks finished before the timed exposure finishes, simply tap the shutter button again to stop the exposure and save the image how it is. **TL**

# The most used Android features and apps

Charles Handmer knows what Android really needs.

We were thinking about how some features and apps become part of your everyday Android life, while others seem exciting at first but soon fall out of use.

Of course, everyone has their own needs, favourites and usage patterns, but in this article we look at the ones that have withstood the test of time and achieved daily use on our devices.

## Spotify - music on demand

Spotify started the music streaming revolution and still dominates, we use it every day – get the app at Google Play Store. The free version of Spotify has ads between songs, but we happily pay $11.99 per month to have virtually unlimited ad–free music anywhere, anytime. There is also a family membership for $17.99 that allows up to six users, and a student membership at $5.99 per month for the first year.

## Synchronised Computer and Android calendars

Back in *TechLife* issue 88 we described how to get cloud–synced Outlook calendars and contacts across all your devices for free. We had been told this was not possible, but it's actually not that hard and we use our synced calendars every day.

Setting it up is too big a subject for this article and you may need to refer to *TechLife* 88, but in simple terms:

1 Create an **Outlook.com** email account.
2 Install the Outlook app on all your devices using your Outlook.com email address.
3 Add your Outlook email to your computer email client and make it the default Data File location.
4 If you use the Windows 10

Grid lines really help the amateur photographer.
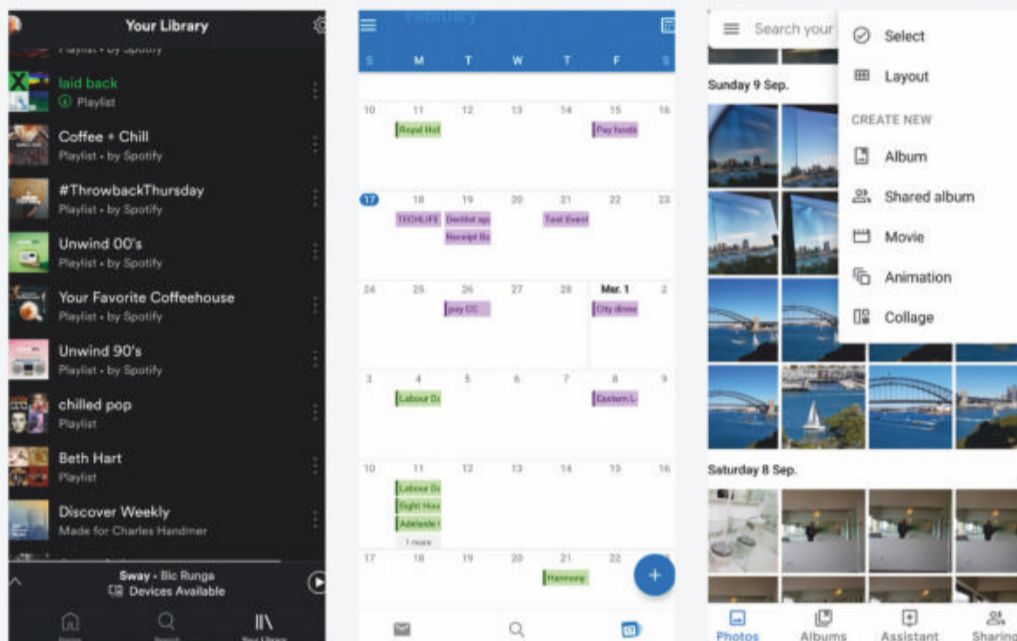
default Mail and Calendar apps, simply add your **Outlook.com** account to the Calendar app (make it the primary account if you have others set up).

5 You now have a Windows calendar that syncs with all your Android device calendars. Any appointments you or anyone else add, change or delete on any device will be synced across all devices when they are online.

## Change your Android keyboard

Google's Gboard is pretty much the default keyboard for Android devices, although Samsung generally uses SwiftKey. We found the SwiftKey autocorrect annoying, so went to the Google Play Store to download and install Gboard. Changing your keyboard is easy.

## Identify and manage app notifications

Notifications on your Home Screen from unknown apps? Just long-press on the notification and your device will tell you. To manage the app tap "Details" or the information icon for direct access.

## Camera grid lines

Of all the camera options, we have found that grid lines are the single most useful feature to help frame, align and compose photos. Check your camera settings to see if you have this feature available.

## Google Photos

Just about every Android device has a camera, and before long thousands of digital photos fill the available memory. You can transfer to a computer or other external storage, or just delete mercilessly, but there is a way to have both your memories and your phone memory. Your device probably already has the Google Photos app installed. Activate it and link to your Google account to access unlimited photo and video storage for free.

Unless you have a big international data allowance, set

Google Photos to upload on Wi-Fi only. Then relax, your photos will be backed up to the cloud as long as you run the app frequently.

You then use "Delete Device Copy" or "Free up Device Storage" on the Google Photos app menu to delete photos on your device but keep them in the cloud. The great thing about this is that all the photos remain accessible on your device – just click to download and view.

## Backup

Google Backup and Restore lets you clone your phone settings, contacts etc. to a new phone if required. It's already installed on your Android smartphone, so just make sure it's enabled.

Go to Settings > Google > Backup (or search for Backup to find it) and make sure "Back up to Google Drive" is switched on.

## Backup Contacts, Call logs, SMS, MMS, System Settings, Applications etc.
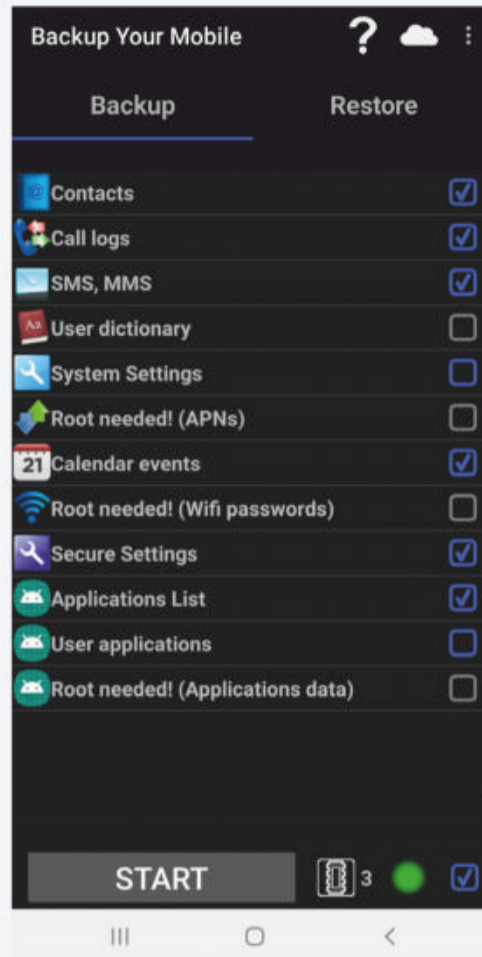
We can rely on Google to backup our Android settings and data, plus photos and videos, and all we had to do was switch the options on. But what about SMS/MMS messages and other contents?

There are numerous apps but our favourite is the basic "Backup Your Mobile" – downloadable for free from the Google Play Store. Backup Your Mobile copies your data into an archive and uploads it to the cloud. You also have the option of setting a daily, weekly or monthly scheduled backup. Just set and forget!

## Speak and read any language

There are a number of translation apps available, but it's hard to do better than Google Translate, which is also downloadable to work offline. Just get the app from the Play Store, set it up, and download the

Backing up to Google is built into your Android device.

Quick settings are just a swipe away, and customisable.

languages you want available.

Apart from text translations, Google Translate does a good job of voice recognition and lets you have (somewhat stilted) conversations in different languages.

There is also the clever camera translation option, that displays approximately translated versions of signs, menus, parking meter instructions, any text in fact. This can be incredibly useful, and sometimes amusing!

## Step Tracker – Pedometer Free & Calorie Tracker

This simple step counter app is very easy to use. Simply install, set your personal profile and preferences, leave your phone in your pocket or bag and it will automatically record your steps, how many kilometres you have covered, how many calories you have burned, and there is an option to track your walks with GPS. It runs in the background and does not need to be active to record.

## The Quick Settings screen

Instead of delving through Settings menus, swiping down twice from the top of the screen,
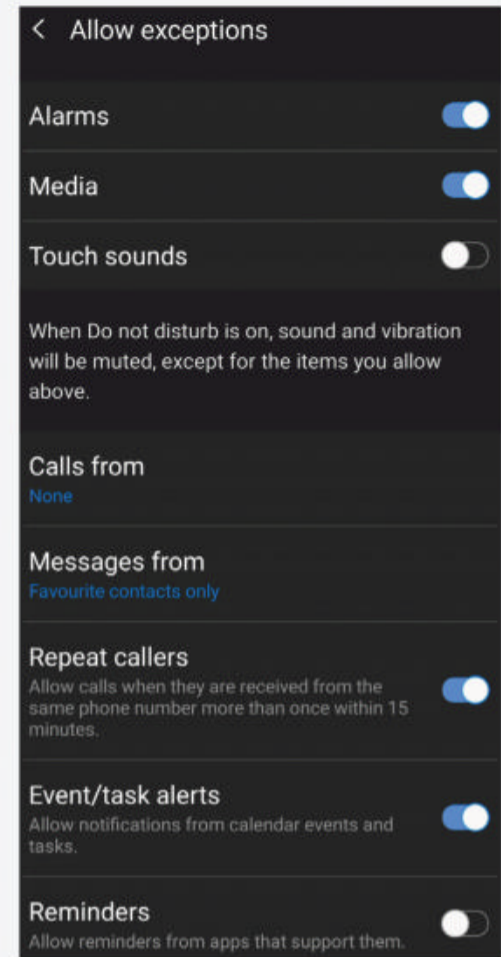
or a single two finger swipe, opens the Quick Settings screen. Tap on the item Icon to toggle it on or off, or tap on the item name below the icon to access its settings.

You can customise the Quick Settings screen too. Tap on the menu icon to access customisation, then you can drag icons around to set up the screen just the way it suits you.

Quick Settings really are quick, and let you do things like:

**Quick Setting – Do Not Disturb** Do not Disturb, or Priority Mode, blocks all interruptions except those you specify in the settings. Just set your preferences and then toggle on and off as required via the Quick Settings screen.

**Quick Setting – Change the Power Mode** Optimise your battery use.

**Quick Setting – Turn NFC on or off** If you use NFC (Near Field Communication) for contactless credit or debit payments you can use the Quick Settings screen to instantly turn NFC off when you don't need it.

**Quick Setting – Save mobile data** Tap on Mobile Data below the icon and you have direct access to mobile data management and data saving settings. **TL**
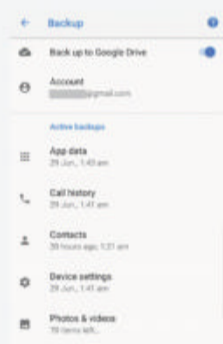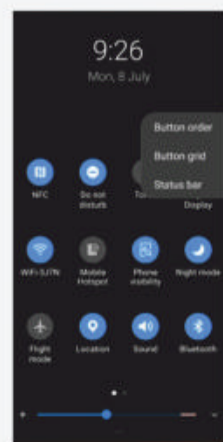
Security & Privacy

# Buying anonymously

Nathan Taylor shows you how to keep your identity safe when purchasing online.

Last month we talked about "burner identities" and some of the ways you can keep your personal information out of the hands of potentially dodgy sites and services. As you might expect, maintaining that anonymity when engaging in financial transactions is somewhat harder. It's not impossible, however, and this month we're going to look at some of the ways you can make online purchases without giving out excessive – or any – personal information.

Obviously in some instances complete anonymity is impossible. If you're getting physical goods delivered you'll need to provide a valid address, for example. Even then, however, there are steps you can take to keep your financial details, at least, private.

## PayPal
**Pros:** Widely accepted, hides credit card details.
**Cons:** Difficult to hide full identity.

One of the simpler and widely accepted tools you can use is an online payment system like PayPal. These generally do not

PayPal is widely accepted and will hide your credit card details.
**FAR RIGHT:** BRD allows you to manage multiple wallets and currencies and is relatively easy to get started.

**BELOW:** Prepaid cards, even rechargeable ones, can limit your risk.
**BOTTOM:** Gift cards can provide complete anonymity.
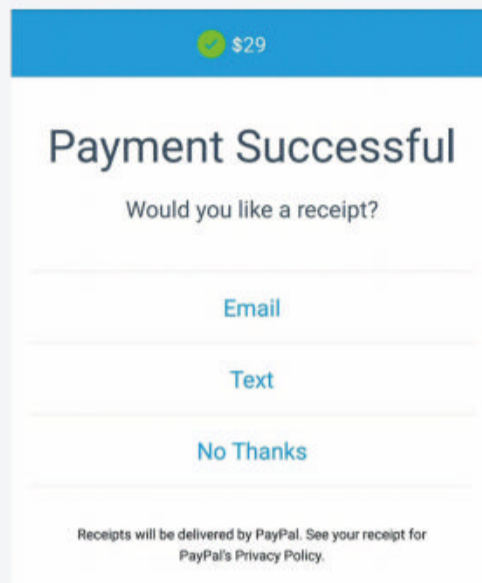






provide any kind of anonymity other than financial. When you make an online purchase with PayPal, for example, the recipient will see the email address and name you used to register the PayPal account. It's difficult to create a 'dummy' PayPal account with fake details, since PayPal requires that you register a valid credit card or bank account with it as a payment method.

What PayPal will do, however, is keep your credit card details safe. It essentially serves as an intermediary – PayPal will make the payment on your behalf, then you pay PayPal. That way, the company you're buying from never gets to see your credit card details; only PayPal does. PayPal also provides purchase protection much like credit cards do: merchants that use PayPal are required to sign an agreement to provide chargeback-style refunds if PayPal determines that the transaction was not completed properly.

## Prepaid
### debit and gift cards
**Pros:** Accepted at most places where credit cards are, gift cards can be purchased completely anonymously.
**Cons:** Purchase cost, some sites will reject them, can be left with unusable money .
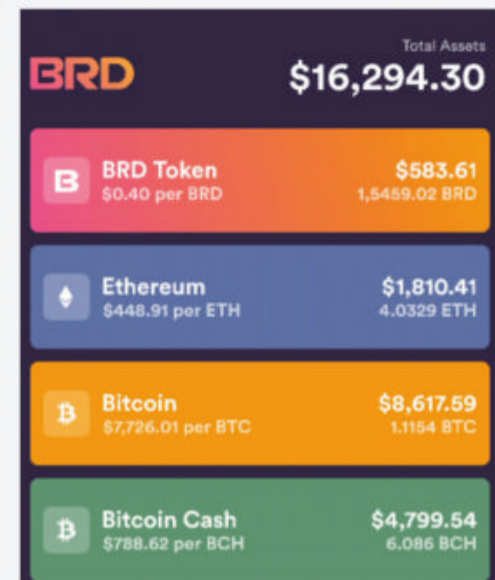
A variety of financial services now offer prepaid debit and gift cards that link to a limited Mastercard or Visa account. These have two possible advantages – there's a hard limit on how much money can be stolen from you at once if your card details are compromised; and it may be possible to purchase them completely anonymously, so that the card is never linked to your identity.

There are two types of cards you can get: a rechargeable prepaid card and a gift card, which can only be used until the money runs out and is then discarded. For anonymity, gift cards make the better option – rechargeable cards might have your name attached to them and you'll likely have to register your details with the card provider in order to provide a recharge method.

One good option in Australia is the Australia Post Gift Card by Mastercard (see **auspost.com.au/money-insurance/prepaid-cards**), which can be purchased in most AusPost outlets, with cash or any other payment method. The card costs $5.95 to buy and can be loaded with up to $500. It will not have a name or identity attached to it – the name on the card will simply be "Gift Cardholder".

The gift card should work at most places that accept Mastercard. However, some sites might reject them, especially for recurring payments like subscriptions. In

addition, gift cards often have the downside of ending up with a small amount of money left over that you can't spend, since any purchase for which you don't have sufficient funds left on the card will simply be rejected by Mastercard, and not many online stores allow you to 'split the bill' into multiple payment methods. If you have a small amount left on the gift card, you can try taking it to a physical store: many friendly physical stores will let you make partial payment for a purchase with the gift card and then make up the difference with cash or another payment method.

## Disposable virtual credit cards

**Pros:** Can very quickly and easily generate a new temporary credit card number .

**Cons:** Still have to trust your financial details to a third party, some require subscriptions to be able to create.

Along the lines of the prepaid and gift cards, virtual credit cards are a way to create 'burner' credit and debit cards that can be used for purchases and then discarded. The difference is right there in the name: a virtual credit card is purely digital – a number you can use to make online purchases, but can't be taken into physical stores.

In most instances, you have to sign up to a service like Revolut (**www.revolut.com**), NetSpend (**www.netspend.com**) or ecoPayz (**www.ecopayz.com**). These services then allow you to generate temporary virtual credit cards that will work wherever Visa or Mastercard are accepted. They're useful for signing up for free trials that demand you provide a credit card number, or for purchasing from sites that don't seem entirely on the up and up.

## Cryptocurrencies

**Pros:** Can be completely anonymous.

**Cons:** Not widely accepted, can be challenging to get started, wildly fluctuating value.

Services like Revolut allow you to generate disposable virtual cards on demand in a mobile app.



The Ledger Nano X, a popular Bitcoin wallet.
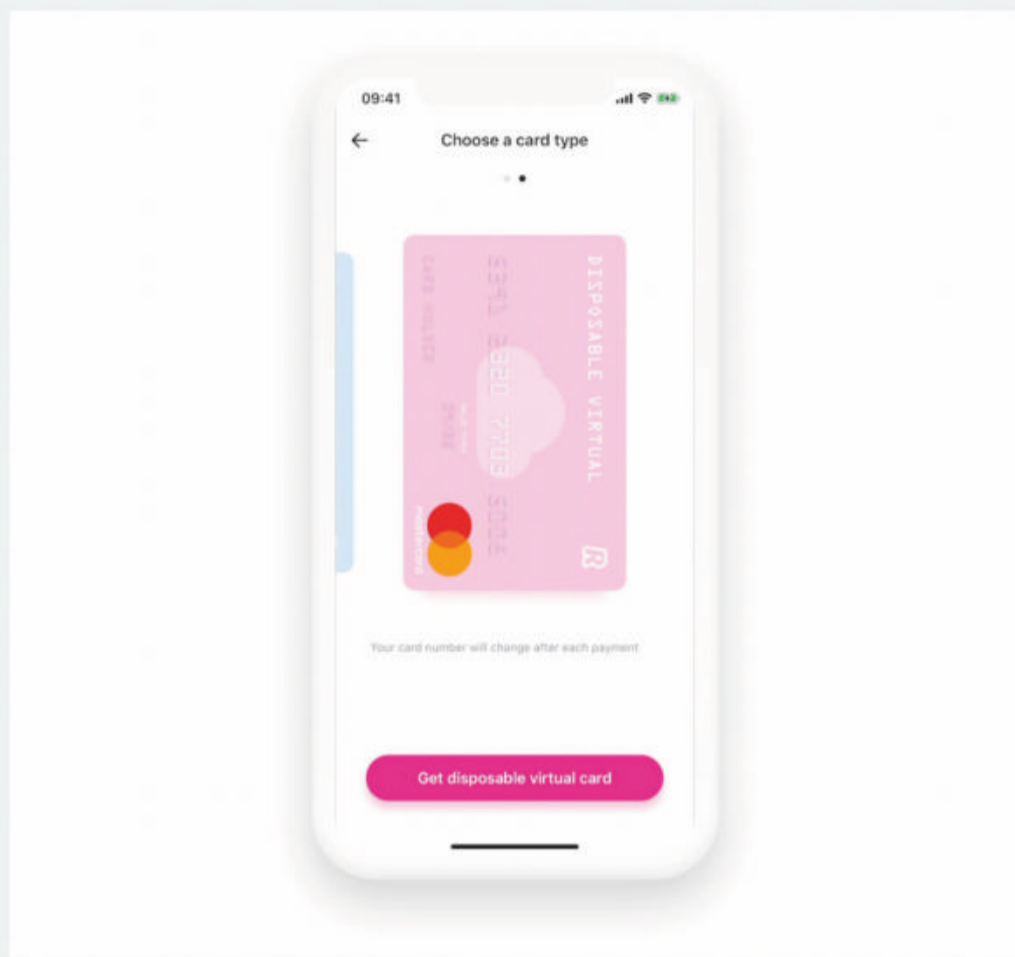
If you want true anonymity when purchasing, then nothing beats cryptocurrencies. Bitcoin and other cryptocurrencies are now accepted by some merchants for digital and physical purchases, and it's entirely possible to make a purchase without giving a single element of your identity to anyone.

The way it typically works with Bitcoin is this: you first create a Bitcoin wallet. Wallets are anonymous – there's no name or other details attached to them. Then you purchase Bitcoins from a Bitcoin exchange and have them sent to your wallet. Then, when you try and buy from a store with Bitcoin, the merchant will provide you with a Bitcoin wallet ID and/or QR code to transfer the Bitcoins to, the number of coins to transfer (which will be based on the current exchange rate) and a time limit in which to send those funds. Then you use your Bitcoin wallet to send the funds to the designated address.

Now this may seem complicated at first – and it is a little – but it can very quickly become second nature once you've got the process down.

The real challenge is initially setting up your own Bitcoin wallet. There's a deep, deep rabbit hole of different options and methods when setting up a Bitcoin wallet. For beginners, we recommend a simple mobile app like BRD (formerly Breadwallet) or the Coinbase app, which are both available on Android and iOS.

You can also look for a physical Bitcoin wallet, a small fob-like device that adds an extra level of security since the Bitcoins stored on it can only be accessed when it's plugged in or connected via Bluetooth/NFC. You still make transactions using your mobile or PC, but you need the wallet device to be there in order for the transaction to work.

Some of the most popular options include Ledger (**www. ledger.com**) and Trezor (**trezor.io**) devices, which are simple to get started with and won't break the bank.

You can purchase coins for your wallet ahead of time or as-needed – though we often recommend the latter to avoid the effects of wildly fluctuating coin values. Then, once you're set up with a cryptocurrency payment system, you'll have the ability to make completely anonymous purchases and avoid giving out any part of your identity to those you transact with. **TL**

# Create your own VPN

Nathan Taylor shows how to keep all your devices connected to each other.

Any user you allow VPN access to will need to have a secure account.

If you've been following along with this column for the last few months, we've been running a series on various types of home servers, and the tools and techniques you need to set them up. This month we thought we'd look at an oft-overlooked but very useful type of home server: the home virtual private network (VPN) server.

What we're talking about here is not what you might be thinking of when you hear 'VPN'. The term VPN is most commonly associated now with commercial, subscription-based VPN services that can be used for security and anonymous access to websites. Those are VPNs run by a third party that you pay to access.

But you don't necessarily have to. It's entirely possible to create your own private VPN on your home network, and that's what we'll be discussing in this column.

## Why a VPN

So the question you might reasonably ask is: why? Why would you set up your own VPN server at home?

The answer to that is actually right there in the name: it creates a virtual private network. Let's say you're away from home, using your laptop or Android phone. Using a VPN, you can 'dial in' to your home network, and then your laptop or mobile will operate and work with your other devices exactly as if it were connected to your home network.

You could, for example, access Windows File Shares or NAS devices. If you have remote access set up on a PC, or Steam or PlayStation local game streaming, then the device could access it from anywhere in the world over the internet. For all intents and purposes, the device will think and act as if it's

**RIGHT:** Add a new incoming connection.

**RIGHT:** Select 'Through the internet' for How people will connect. Yes, it's still an option to use a dial-up modem to connect.

**FAR RIGHT:** You can leave the defaults.
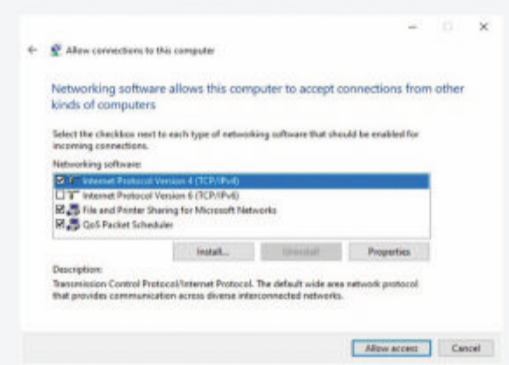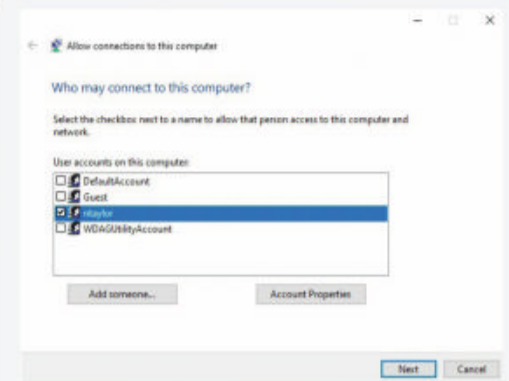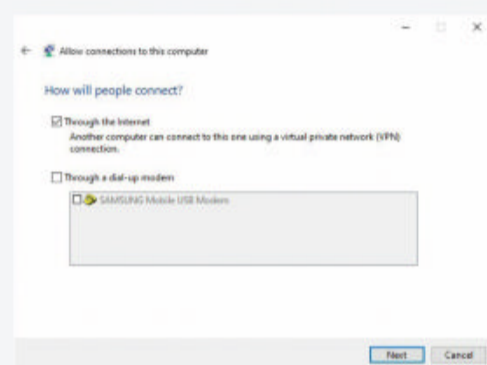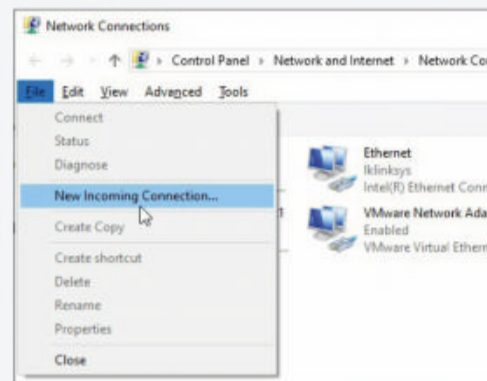
connected to your home network, even when you're on the other side of the world.

It also provides some security. The device will route its internet traffic through your home internet connection. It will still use its own internet quota to connect back to your home network, but outgoing internet connections will be routed back through your home network, and any security measures you have in place on your home network will be applied.

The link, or 'tunnel', from the device to your home network is encrypted, and that also provides some security. If you're using a public Wi-Fi hotspot, it will protect your connection from listeners, the exact same way that a commercial VPN service will.

## Other VPN software

While the Windows VPN service is easy to get up and running (which is why we covered it here), it's very limited in its capabilities and security models. There are plenty of third party alternatives, however. On the more technical end, you can try OpenVPN (**openvpn. net**) or strongSwan (**strongswan.org**). If you need something a little more accessible, try WireGuard (**www.wireguard.com**) or SoftEther VPN (**www. softether.org**).

## Setting up a Windows 10 VPN server

Thanks to the built in VPN in Windows, setting up a server at home is actually relatively easy, with no extra software needed. Just follow these steps:

In Windows 10, go to Settings > Network & Internet.

Click on Change adapter options. This will bring up the Network Connections window.

In the Network Connections window, tap on the Alt key to bring up the drop down menus. Then select File > New incoming connection.

You'll be asked which users of this PC will have access to this VPN, and given a list of current users. This is critical – only choose a real user (not Guest or DefaultAccount), and that user must have a good password set up. The VPN will use that user's Windows login credentials as the username/password for the VPN, and a poor password could make your home network extremely vulnerable to attack.

You'll be asked which protocols to allow. The default (IPv4, File and printer sharing, QoS) should suffice for most users. Click on Allow Access.

Finally, the VPN will be enabled, and you'll be given a computer name that you should make a note of.

You'll see in the Network Connections window that a new 'Incoming connections' device has been created. You can right click on it to change the properties or delete it at any time.

And that's it – a basic VPN server has been set up. Next, we need to set up our router to accept incoming connections.

## Setting up the network

As we've covered this in previous months, we won't go over all this ground again. But there are basically one to three things you need to do:

Fix the local IP address of the computer you're using as the VPN server. This allows port forwarding to function. We provide a full guide in the *TechLife* February 2020 Home Networking column.

Set up DDNS. This allows the VPN to be connected to with a fixed URL like TechLifeVPN.ddns. net. For a full guide, see *TechLife* January 2020's Home Networking column.

Set up port forwarding from the router to the VPN server. You can find a full guide in *TechLife* March 2020's Privacy and Security column or at **portforward.com**. For the VPN, you need to forward port 1723 to the IP address you set up for the server in step 1 above.
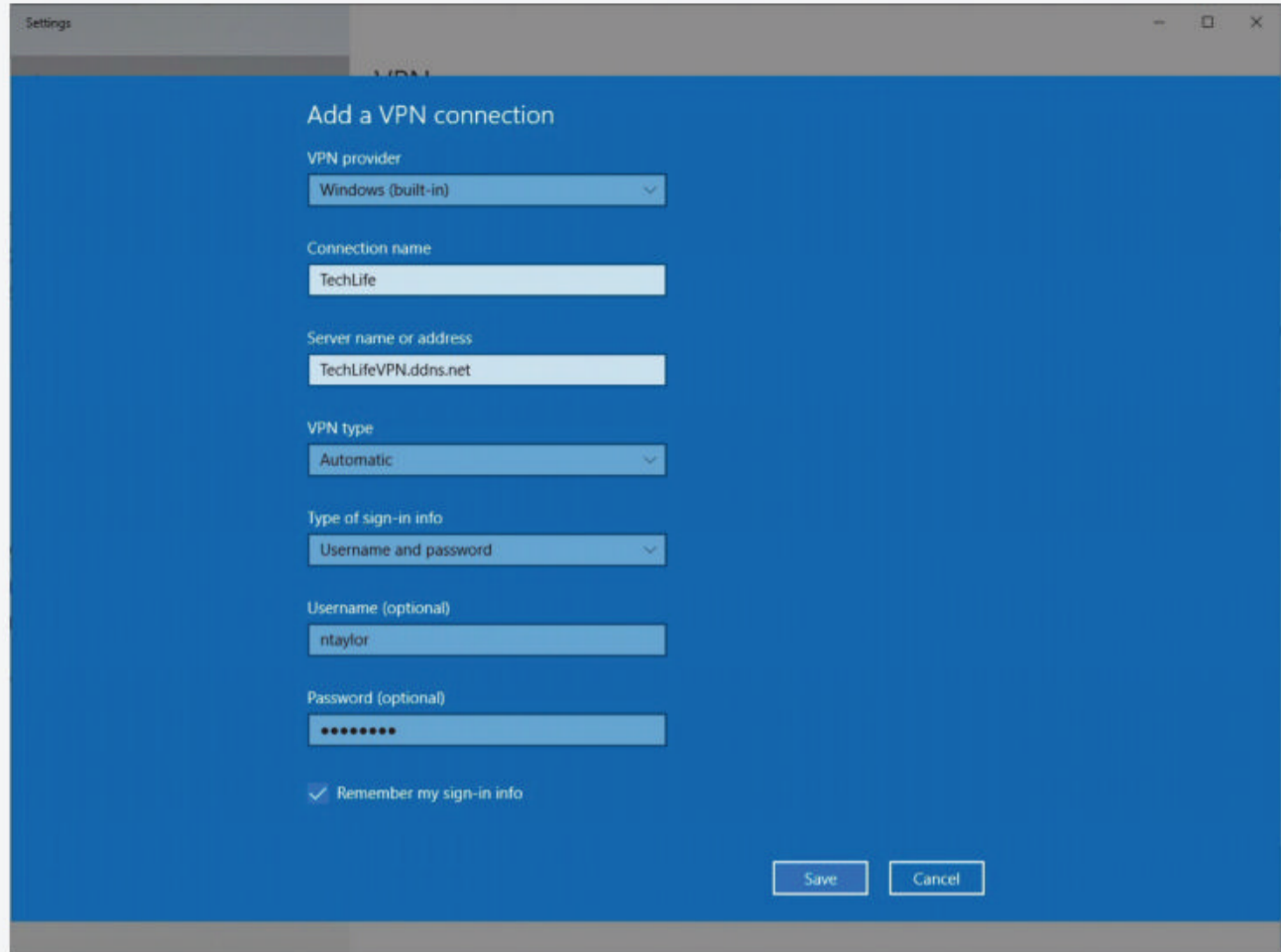
## Connecting to the server

Now that your server is up and running, it's time to connect to it from the client devices. You should be able to connect to it from anywhere on the internet using just about any device that supports PPTP VPN connections.

If you're trying to dial in from a Windows PC, go to Settings->Network & Internet and select VPN from the left panel. Click on the '+' to add a new VPN connection, and enter the details for the connection: give it a name (this is just a local identifier and can be anything), the server's internet IP or DDNS address, and the username and password for an authorised user. Once you've done that, a new VPN connection

**ABOVE:** Windows 10 has made it quite easy to make a new VPN connection.

**ABOVE:** Creating a VPN profile on Android..

**BOTTOM:** Make a note of the computer name.

will appear in the list of available connections – click on it to connect or disconnect at any time.

On Android, it will vary a little from device to device. But generally you'll go to Settings > Connections > More connection settings > VPN. Click on the vertical ellipsis to add a new VPN profile. Give it a name and enter the address. When it comes to the protocol, Windows VPN now actually supports a variety of connection protocols – but for simplicity you can just use PPTP. It's not the most secure protocol, but it's sufficient for most users, and doesn't require any additional configuration. Once you've created the profile, just tap on it to activate it.

Unfortunately iOS no longer supports PPTP, making it much harder to connect. If you want to use iOS, we recommend using a third–party app (see the Other VPN software sidebar).

Once connected, you should be up and running. You should be able to access the services on your home network, and use the device exactly as if you were connected to your home network – which, from the perspective of the device, you are. **TL**
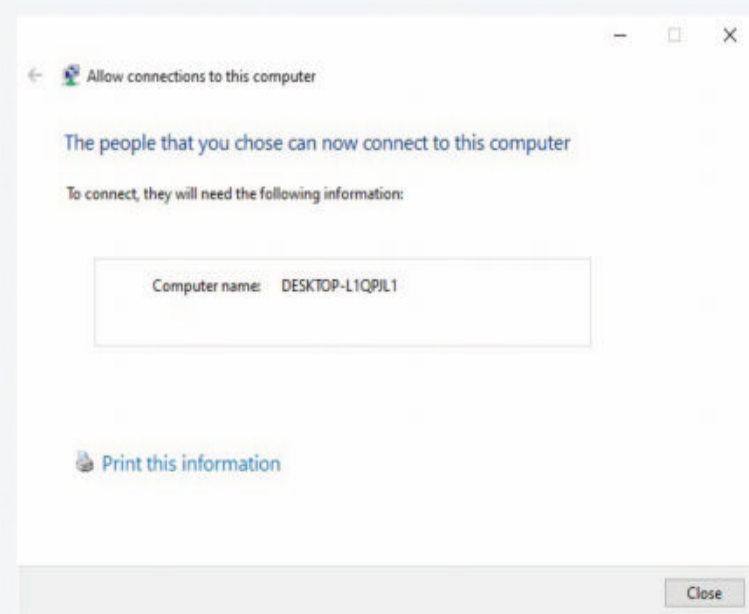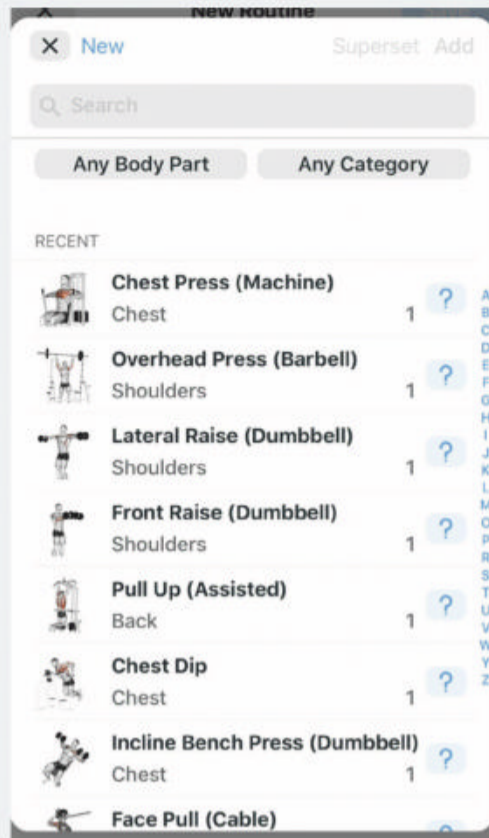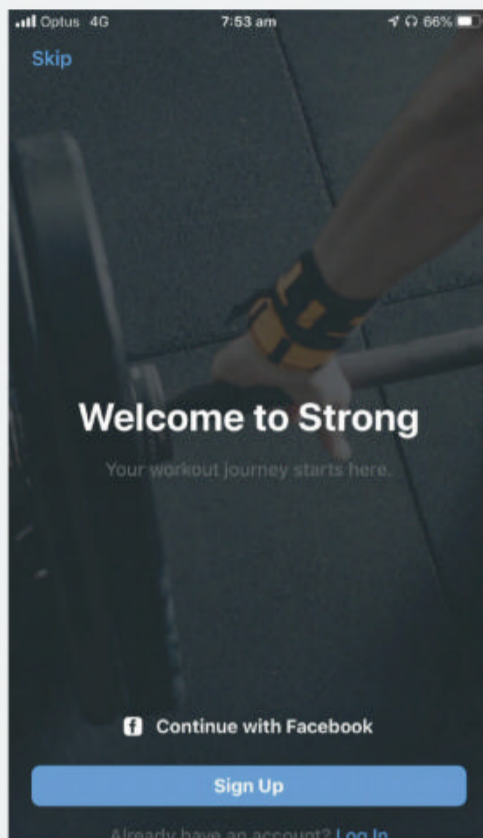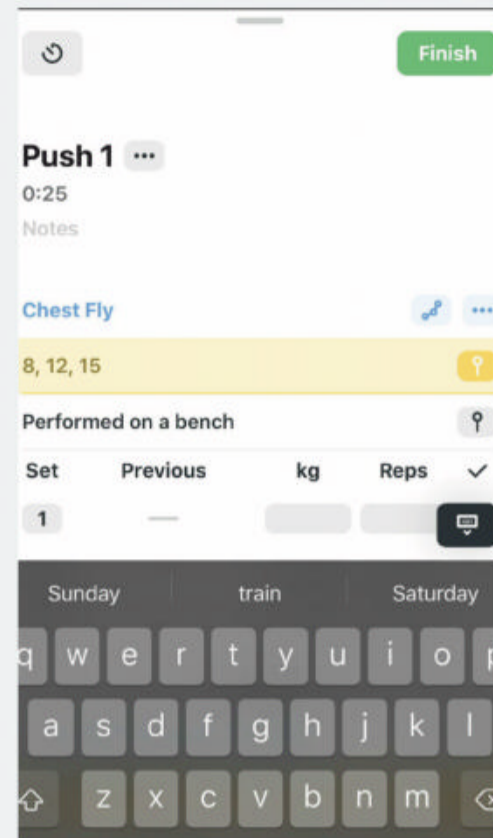
**FAR LEFT:** Start by creating a new account.
**LEFT:** There's hundreds of exercises to choose from.
**RIGHT:** Tap the pin icon to make notes sit permanently alongside an exercise or workout routine.

# Strong

Get strong with Strong.

Sure, working out is often associated with the goal of losing weight, but exercise offers so much more than just shedding a few kilos. Whether you're diving into the pool or hitting the gym floor, one of the biggest draw cards of working out is the ability to see improvements long-term. Given this is especially true when it comes to 'pumping iron' at the gym, this month we're taking a look at Strong – an app that allows you to track weight and reps across a wide range of exercises. Here we'll walk you through the steps to setting up and tracking workout routines, plus show you how to monitor your progress over time.

## The basics
**Getting started.** To begin, download the Strong app from either the Apple or Android app store and pick the option to create a new account. Strong can be used across all your devices, with every workout synced to the cloud. During registration you'll be encouraged to subscribe to the premium version of the app – while there's some great features on offer here, we'd recommend holding off until you get familiar with the app to determine whether it's something you actually need.

**Creating a workout.** Before hitting the gym, you'll want to create a workout. To set up a new program, tap +Routine on the Start Workout tab and give it a name. The app has hundreds of strength- and cardio-based exercises, each with step-by-step instructions and videos. In addition to using the search tool, you can also browse exercises by category or body part. To create a superset (which involves performing multiple exercises in succession), choose the exercises you want to include before tapping the Superset option displayed in the top-right corner of the screen. When adding exercises, you can also specify the number of sets and reps to be performed. Note that the free version of Strong allows you to have a maximum of three routines saved in the app.

> *Whether you're diving into the pool or hitting the gym floor, one of the biggest draw cards of working out is the ability to see improvements long-term.*

**Workout tracking.** Now it's time to begin your workout. After selecting a routine from the New Workout tab you'll be taken to a page listing every exercise to be completed. At the end of each set, simply enter the weight and reps into the appropriate boxes. You can also tap the name of an exercise to see instructions and a history from past workouts. In addition to ordinary sets, there's the option to add a warm-up, failure or drop set by tapping the set number displayed below a particular exercise. At the end of your routine, tap Finish to see a summary of your workout, plus any new PBs.
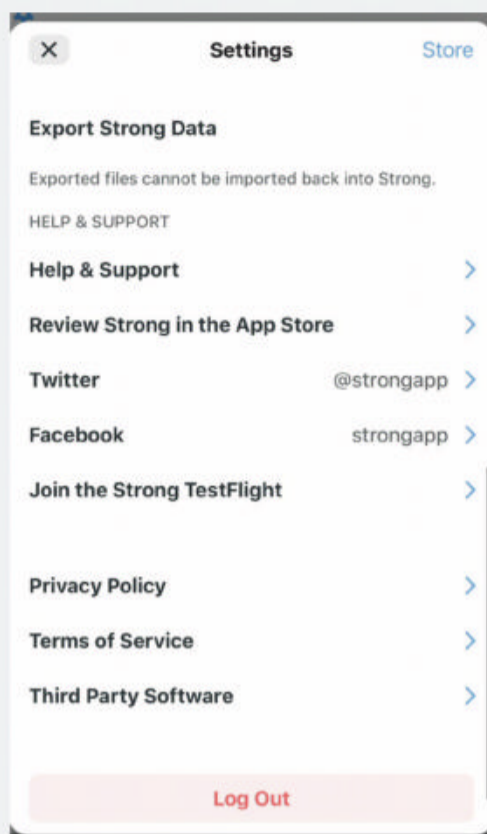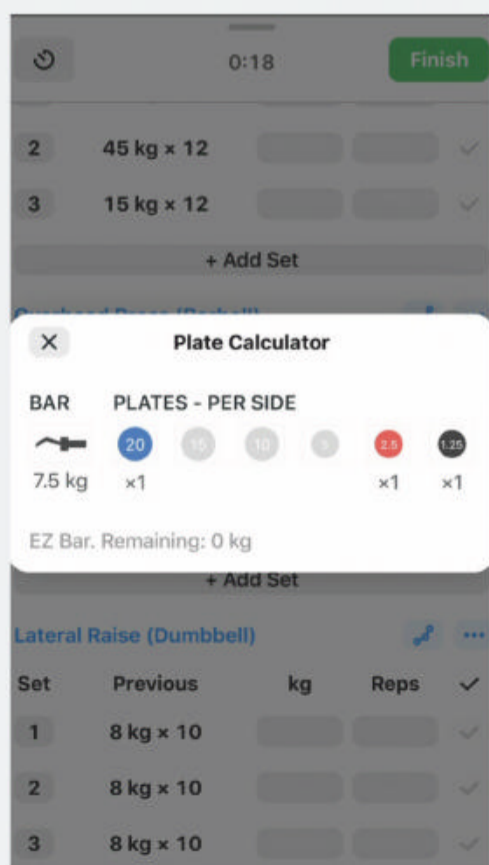
## Step it up a level
**Notes.** As you progress through your workout, there may be times when you want to add a comment. For example, if you used a different piece of equipment, or felt weaker on a particular exercise. Strong allows you to add notes by tapping the ellipsis icon next to an exercise and selecting

Add a Note. By default, notes will appear in the history section of an exercise but won't roll over to future workouts – for this to happen you'll need to tap the pin icon to make it attach permanently to an exercise. You can also add notes to entire routines.
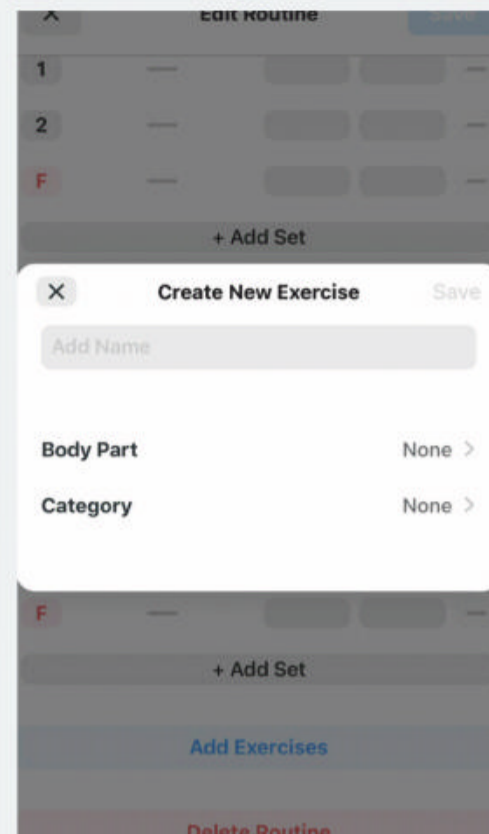
**Calculators.** Warming up is an important part of any workout. Available to premium users is a calculator that uses your past performance of an exercise to suggest weights for a warm-up set. You can access this tool during your workout by tapping the ellipsis icon next to an exercise and selecting Add Warm-up Sets. Premium users can also use the app's handy plate calculator to quickly determine what plates are required to reach a certain weight. The plate calculator is located on the keyboard.

**Timers.** Keeping track of time spent resting between sets and exercises is easy thanks to the timer tool. After completing a set, simply tap the timer icon in the top-left corner of your screen and pick a duration. When building a new workout you can also create auto-timers that start immediately after logging each set — this can be done by tapping the ellipses icon and selecting Auto Rest Timer.

**Results.** Strong makes it easy to see improvements over time. In addition to charting weight and reps across workouts, the app keeps track of maximum volume and weight, plus your one-rep max (1RM). If you choose to sign up for a premium subscription, you can also see your progression plotted visually on a graph.

## Step it up a level

**Custom exercises.** If you have an exercise that's not in the app, you can add it yourself. While adding exercises to a new workout, tap New to be taken to a page where you can enter a name, body part

**LEFT:** Export your data to a handy CSV format.
**RIGHT:** If an exercise isn't in the database, you can add it yourself.

and category. Custom exercises are stored in the app's database ready for adding to future workouts.

**Exporting.** Not confined to the Strong app, you can export your workout data in a CSV format. To do this, tap the settings cog displayed on the profile tab and select Export Strong Data. Note that while you're able to export information out of the app, there's currently no way to import workout data. Strong can also integrate directly with the Apple Health app, along with connect to your MyFitnessPal account for calorie syncing.

**Smartwatch support.** Prefer to leave your smartphone in the locker? If you own an Apple or Android smartwatch, you can view workouts plus enter weight and reps for sets, all from your wrist.

**Body measurements.** In addition to tracking workouts, as a premium user you're also able to keep tabs on how your body is changing over time. Strong lets you track a wide range of body parts including calves, thighs and biceps, along with your weight and body fat. You can do this from the Measure tab. **TL**
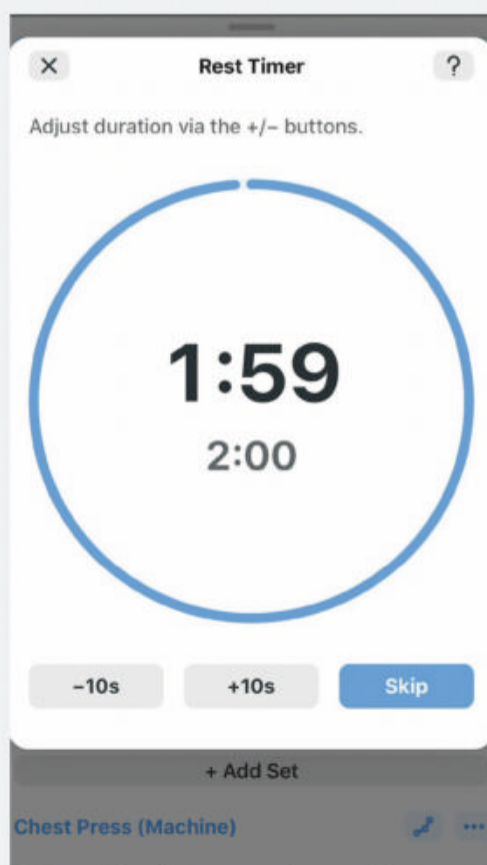
**FAR LEFT:** The plate calculator is great for quickly determining what plates are required to reach a certain weight.
**LEFT:** Set a timer to begin automatically after logging each set.

# Enhance reflections

Use a circular polarising filter for the less-known application of creating strong reflected images in landscape scenes.

Polarising filters are often seen as a staple item in the landscape photographer's kitbag. They are essential tools for boosting colour saturation in an image, increasing contrast and reducing reflections – one of the most well-employed applications for these items.

A polariser works by differentially permitting light into the lens, dependent on its orientation. Reflected light is highly polarised, so by aligning the mesh of the filter to the angle of those rays (reflected off a lake surface, for example) more reflected light is filtered compared to the light coming from the surroundings.

However, a less commonly known application of a polariser is to increase the brightness of reflections. By rotating the filter to align the structure with non-polarised light in a scene, the native light-reducing properties of the filter appear to apply more to the surroundings than to the source of the reflection.

While a filter will never 'increase' light transmittance, the relative difference in filtration effect, for example between the lake and the surrounding land, is reduced – the reflected images therefore seem closer in brightness to the real-world scene elements.

While this may seem a complex scenario, in practice a photographer can enhance reflections by learning how their filter behaves in different settings. Here we'll walk through the process that's involved.

**After**
BRIGHTER BALANCE
By correctly employing a polarising filter, the differential brightness between real-world and reflected images is less pronounced, increasing reflection visibility and creating greater landscape depth.
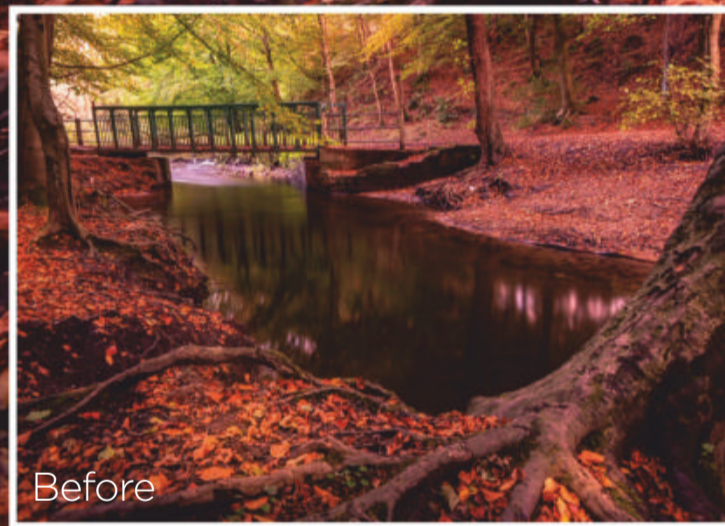
Before

**1** ATTACH THE FILTER A circular polariser has a filter factor of 3 to 4, meaning it will cut light by up to 2 stops. Therefore it is best to attach the filter before attempting to calculate exposure using AE modes.

**2** COMPOSE YOUR SHOT In darker environments use a camera support, due to the light reducing the filter properties. Find an angle that will show the reflection to best effect, for example to mirror the landscape.

**3** CUT REFLECTIONS Start by rotating the filter until the reflections disappear almost entirely. This will help you to find the position of the lowest reflection-enhancement, from which to produce the inverse filter effect.

**4** FIND THE STRONGEST EF-FECt Rotate the filter ring while observing the reflection through the viewfinder. Turn it slowly until the reflected image appears strongest relative to the rest of the scene. Hold this position.

**5** CALCULATE EXPOSURE Take a meter reading from the reflected area to create as bright an image as possible. Use an aperture setting of at least f/11 to ensure sufficient depth of field in the reflection and surrounding scene.

**6** ADJUST YOUR ANGLE The camera angle relative to the sun also impacts on the apparent strength of the filter effect. Try moving around the scene to experiment with how your position adjusts reflection visibility **TL**

**INSET:** Before
**MAIN:** After



# Hue/Saturation control & mastering it

Get to grips with one of the best Photoshop tools for boosting and altering colours.

At first glance, the colours in an image can sometimes look disappointingly flat – and nothing like how you remember them when the shot was taken. If you want to give those dull colours a quick boost, one of the easiest edits to make is a simple increase in saturation.

This is where Photoshop's Hue/Saturation command comes in. You can use the command to increase saturation, either across the entire image or by targeting specific colour ranges. In my paint image, for example, I can enhance the greens in the paint to give the image a much-needed boost.

The Hue/Saturation command is one of the most useful colour tools on offer in Photoshop. On the face of it, the command looks very simple – but look closer and you'll find plenty of hidden depths. As well as boosting existing colours, the command also lets you change them completely by altering the Hue setting. This is often best carried out on individual colours, which is easily achieved with the handy on-image tool found within the command. If you like, you can go on to adapt colour ranges, add a full colour wash, or make the edit work selectively over your image…
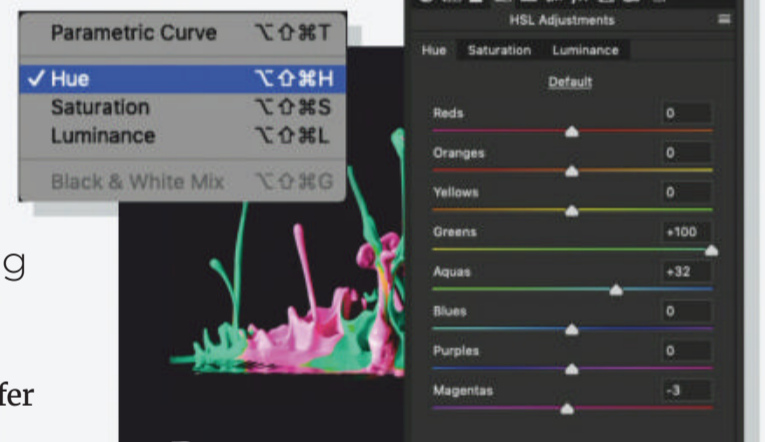
## Raw saturation tools

In the paint image here, I've used the Hue control to completely change the colour of the vibrating paint. But more often than not, the command is used to boost existing colours by increasing Saturation, which results in greater colour intensity. However, this is by no means the only colour-boosting tool on offer. The Camera Raw/Lightroom dialog offers a similar Saturation slider. Then there's Vibrance, which targets the less-saturated colours in the image – useful when some colours lack punch. You'll also find the Targeted Adjustment Tool in the Camera Raw/Lightroom toolbar, which allows you to selectively alter saturation in eight colour ranges.

> " *You can use the command to increase saturation, either across the entire image or by targeting specific colour ranges.*

**1**

HAND TOOL The Hand Tool gives you on-image control over colours. Toggle the tool on, then drag over specific colours in the image to alter the saturation of the targeted colour range. Hold Ctrl/Cmd and drag to target the Hue instead of the Saturation. Here, targeting the hue enables us to change the colour of the green paint splashes, giving swift access to other colours for an entirely different look.

**2**

RANGE DROPDOWN As well as 'Master', which targets all colours at once, you can use this drop-down to target six individual colour ranges: reds, yellows, greens, cyans, blues, magentas. (You can fine-tune the range further – see tip 6.) You can tweak the Hue, Satura-tion or Lightness of certain colours while leaving others unaffected – useful not just for altering the paint colours here, but for all kinds of colour adjustments.

**3**

ADJUSTMENT LAYER AND MASK Here we've applied Hue/Satura-tion as an Adjustment Layer, which means the adjustment affects the layers below it in the stack. You can apply Hue/Saturation directly to a pixel layer by going to Image > Adjustments, but an Adjustment Layer gives greater control: you can edit the settings at any time, or use a Layer Mask to make it work selectively over the image.
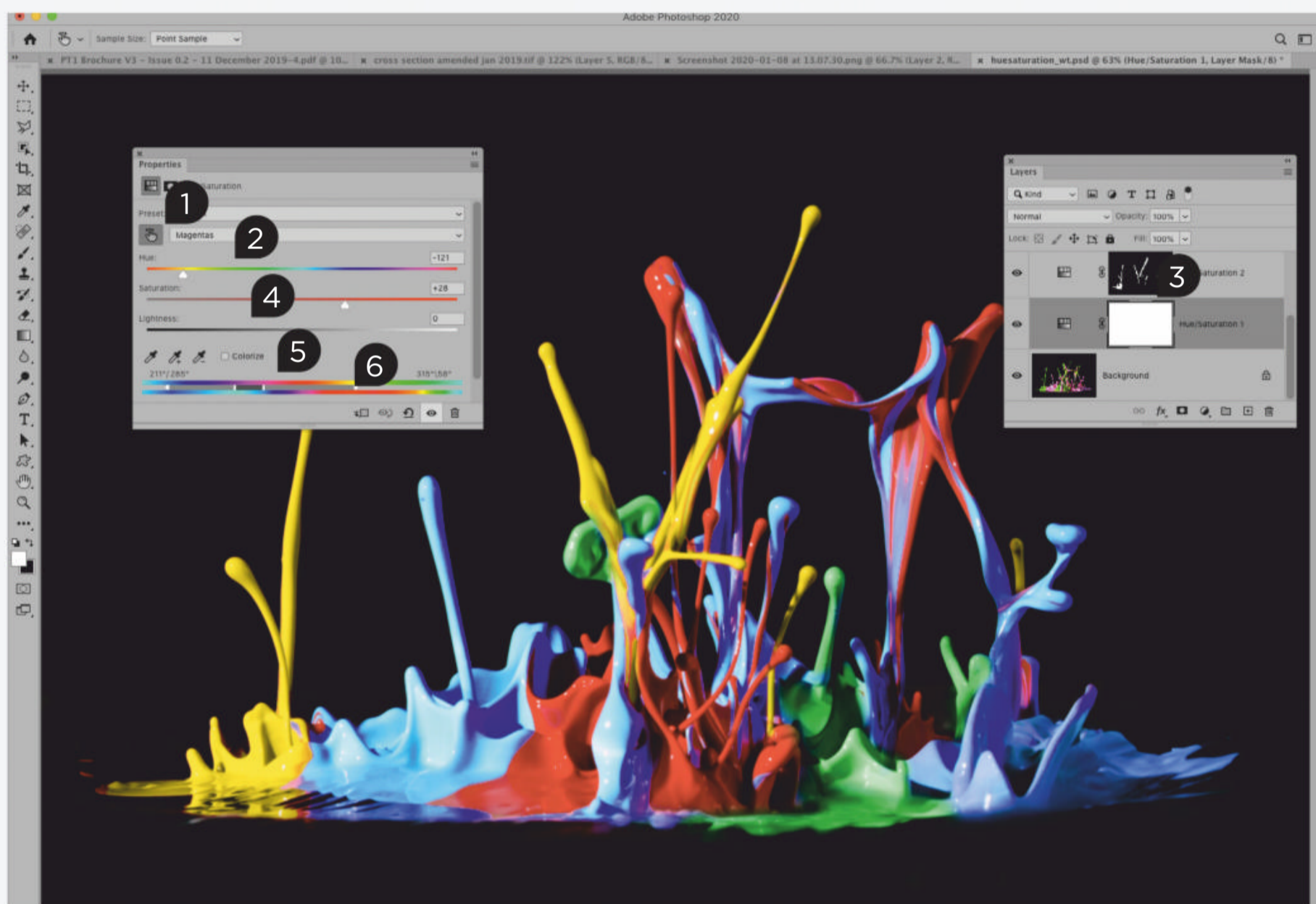


**4**

COLORISE Tick this box to add a col-our wash over the entire image. The initial colour reflects your foreground colour in the colour picker. Adjust Hue and Saturation to alter the colour wash. This can be a simple, effective way to add a colour tint to a black-and-white image. If you use the Color-ise control in combination with a low layer opacity, it gives you the option to add a subtle colour shift to a colour image.

**5**

HUE AND SATURATION SLIDERS The Hue slider alters the colours in your image. Beginning at 0, the slider ranges from +180 to -180. As these fig-ures suggest, it can be useful to think of the Hue slider in terms of a colour wheel, and changes to it as degrees of rotation. Saturation controls the intensity of the colours. Drag right to boost colours, or left to desaturate them. Lightness adjusts the brightness of the colours.

**6**

ADAPT RANGES When you target a colour range (see tip 2), you'll see four controls that let you adapt the range of the affected colours. The two inner bars (the straight lines) control the spread of colours targeted, while the outer trian-gular bars change the fall-off. You can also add to or subtract colours from the range with the eyedroppers. If a range is adjusted into a different part of the spectrum, the list of colour ranges in the dropdown reflects this. **TL**

# SPECIAL OFFER

Subscribe to *TechLife* & save.

## Subscribe to TechLife & save!

Get the next generation of tech magazine delivered directly to your door every month!

Subscribe to *TechLife* and become part of Australia's most exciting technology title. We'll keep you up to date with all the ways modern tech can improve your life, focusing on practical news, reviews, guides and tutorials rather than on specs and gigahertz. *TechLife* isn't just for the geeks: it's for everyone!

Save 34%

## 12 issues for $79

Just $6.58 per issue!

Save 42%

## 24 issues for $136

Just $5.79 per issue!

## Hurry! Offer ends May 4th 2020

Don't wait! Visit **techmags.com.au** or call (02) 8227 6486 to subscribe to TechLife magazine.

Terms & conditions: This offer expires May 4th 2020 and is available to subscribers within Australia only.
Please allow 6–8 weeks for delivery of your first issue. For full terms and conditions, see subscribe.techmags.com.au/style/images/FutureTC.pdf. Please see our privacy policy on page 6.

## SMARTPHONES

### APPLE IPHONE 11 PRO

**From $1,749, apple.com/au**

Packing the best screen and camera on any phone, plus the fastest processor and a beautiful high-quality build, and you've got a phone that earns its Pro name. It's a totally polished package.

### SAMSUNG GALAXY S10+

**From $1,499, samsung.com/au**

A premium build, incredible Infinity-O screen with HDR10+, brilliant rear triple camera system and blazing performance in Samsung's slick new One UI make this the Android king.

### HUAWEI P30 PRO

**From $1,299, huawei.com**

A revolutionary 5x optical zoom (with 10x lossless hybrid zoom) meets a 6.47-inch OLED screen, big battery, and ultra-fast processor for one of the smartest Android phones available.

### ONEPLUS 7 PRO

**From $829, oneplus.com**

With a world-first in screen tech and the fastest wired charging you'll find, this is an ambitious phone, designed to prove that OnePlus can make higher-end flagships as well as mid-range marvels.

## VALUE SMARTPHONES

### SAMSUNG GALAXY S10E

**From $789, samsung.com/au**

The modestly sized and pocket-friendly 5.8-inch screen on the S10e is a breath of fresh air. With Samsung's impeccable levels of fit and finish, great software and top specs, it's a deal.

### MOTOROLA ONE ACTION

**From $289, motorola.com**

One of the most exciting budget smartphones to have launched in... forever. There's a massive 6.3-inch LCD screen on the front, a triple camera on the rear and 128GB of storage inside.

### GOOGLE PIXEL 3A

**$649, store.google.com**

64GB of storage, always up-to-date Android with no extra cruft, snappy performance and a truly brilliant camera, all in a package that defines 'cheap and cheerful' – it's great value.

### HONOR PLAY

**From $485, hihonor.com**

Pitched as a gaming phone, but it's just an all-round brilliant Android phone that's a stone-cold bargain. It has a high-end processor, 6.3-inch screen, good rear cameras and a fantastic design.

## SMARTWATCHES

### APPLE WATCH SERIES 5

**From $649, apple.com/au**

This truly straddles the line between tech and fashion; it's not just the best-looking smartwatch, but its health and fitness features, always-on screen and good apps make it essential.

### SAMSUNG GALAXY WATCH ACTIVE

**From $299, samsung.com**

Sleek and powerful, this is the best smartwatch for Android users. The screen and design are on par with the Apple Watch, while a collection of new watch faces give it a modern edge.

### SAMSUNG GALAXY WATCH

**From $399, samsung.com/au**

The circular screen with innovative rotating bezel is the best way to control a smartwatch, and the slick Tizen software is easy to use. It looks good too, and a battery life of up to six days is ace.

### FOSSIL SPORT

**From $249, fossil.com**

Fossil's fourth generation of smartwatches serves up what's probably the best Wear OS smartwatch available to buy today. Capable and wearable, with good app support.

# BUYER'S GUIDE

The best of the best

## NOISE-CANCELLING HEADPHONES

### SONY WH-1000XM3

**$539, bluesound.com**

With 30-hour battery life, very quick charging, Google Assistant, amazing bass response and an incredibly clever noise cancellation processor, these are superb headphones.

### BOWERS & WILKINS PX

**$399, bowers-wilkins.com**

With useful motion-sensing features, the stylish PXes have variable noise cancelling and accurate B&W sound. We think the Sonys are slightly better, but you may well disagree.
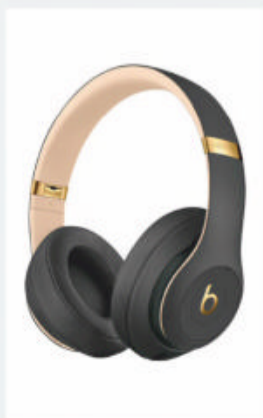
### SONY WH-1000XM2

**$389, sony.com.au**

With the XM3 model replacing these, you might be able to find them cheap – and if you can, you'll get impressive noise cancellation and brilliant sound in a comfortable body. They're still ace.

### BEATS STUDIO3 WIRELESS

**$399, apple.com/au**

These Beats deliver exceptional noise cancellation that reacts very well to all kinds of environments, they get three hours of charge in 10 minutes and they're the best sounding Beats so far.

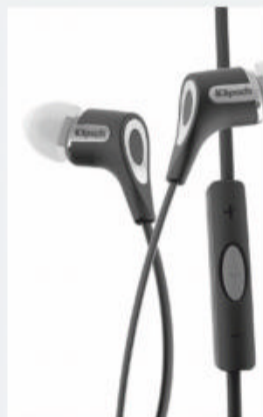## WIRED IN-EAR HEADPHONES

### FLARE AUDIO FLARE PRO 2HD

**$644, flareaudio.com**

These are both wired and wireless – the in-ear bit has a cable to a DAC box, which you can then play music through over Bluetooth or by plugging in. The sound is fantastic – huge and nuanced.
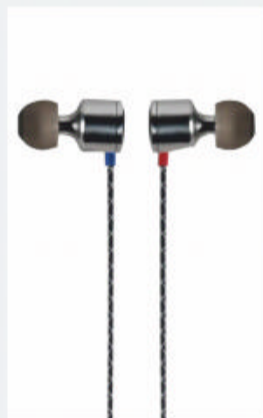
### KLIPSCH R6I II

**$99, klipsch.com**

A more comfortable alternative to in-ear monitors, the R6i IIs deliver lots of bass and a lively, engaging sound. It's maybe a little bass-heavy for older music, but it's great for modern stuff.

### FLARE AUDIO FLARES JET 3

**$164, flareaudio.com**

Maintaining the quality of the Flares Pro (see Bluetooth headphones), removing the DAC element and thereby slashing the price, these audiophile in-ear headphones are a tremendous option.
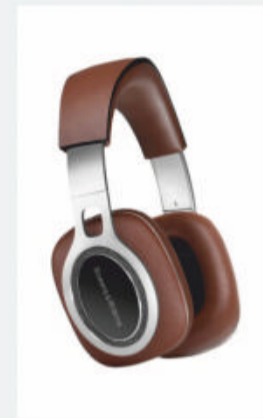
### SOUNDMAGIC E11C

**$99, soundmagicheadphones.com**

Can we really be recommending a pair of headphones for under $100? Yes we can! The grown-up sound quality and exemplary comfort of the 11c make them the sonic bargain of the year.

## WIRED OVER-EAR HEADPHONES
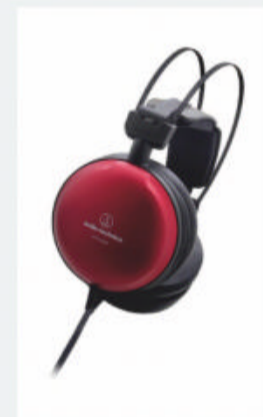
### BOWERS & WILKINS P9 SIGNATURE

**$1,249, bowers-wilkins.com**

The P9s don't just sound wonderful with hi-res audio. They do a stellar job with poor quality music, such as compressed MP3s. You can have any colour you like as long as it's brown.

### AUDIO TECHNICA ATH-A1000Z

**$700, audiotechnica.com**

Forget about MP3s or EDM: these headphones don't flatter or sacrifice sound quality for bass. But if you give them a good amp and a good sound source they do incredible things.
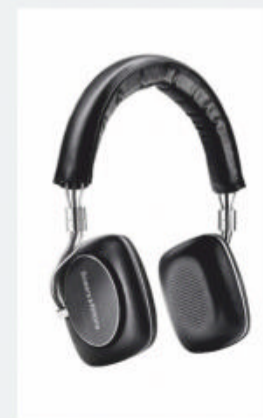
### SENNHEISER MOMENTUM 2.0 AROUND EAR

**$328, sennheiser.com**

The best sub-$350 over-ear headphones aren't too picky about sonic sources. They don't quite have the frequency range of our more expensive picks but they're well built and good for the price.

### BOWERS & WILKINS P5 SERIES 2

**$199, bowers-wilkins.com**

The little sisters of the mighty P9s deliver a beautifully warm and spacious sound for a lot less money, and their closed backs mean they're less likely to annoy other people when you commute.

## LAPTOPS

### DELL XPS 13

**From $1,698, dell.com**

The Dell XPS 13 is thinner and more powerful than ever. Up to 1TB of SSD storage, 16GB of RAM, a 4K screen and fast Intel chips help make it a top quality all-rounder.

### MICROSOFT SURFACE BOOK 2

**$1,757, microsoft.com**

Available in 13- or 15-inch sizes, with a 3:2 screen that gives you more height than other laptops, and plenty of power, this is a light and fast machine that's also really flexible.

### HUAWEI MATEBOOK X PRO

**$1,993, consumer.huawei.com**

This marries style and function, delivering incredibly capable internal hardware in a form factor that also matches Apple's MacBook range in terms of looks and feel.

### ALIENWARE AREA-51M

**From $3,999, alienware.com**

A gaming laptop packed with power, from the ninth-gen i7 processors, to the newest Nvidia mobile GPUs. The performance you get back is worth the substantial outlay.

## 2-IN-1 LAPTOPS

### MICROSOFT SURFACE BOOK 2

**$1,757, microsoft.com**

Pull the screen away from the keyboard and it's a tablet. Connect them for more graphics power and battery life. A premium, fantastically portable, and supremely versatile system.

### HP ENVY X2

**From $899, hp.com**

The big sell here is the monstrous battery life, with up to 22 hours on one charge. This is because it makes use of ARM architecture, with a Snapdragon 835 CPU powering everything.

### DELL XPS 15 2-IN-1

**From $2,549, dell.com**

With a big screen and great specs, what's not to like about this 2-in-1? Well, the price is steep, but if you can afford it then this is undoubtedly one of the best touchscreen options.

### ASUS ZENBOOK FLIP 13

**$1,299, asus.com**

The Zenbook Flip 13 might be the best laptop Asus has ever released. Tooled up with an eighth-gen Intel Core processor, the tablet mode feels great to use, thanks to a responsive touchscreen.

## TABLETS

### APPLE IPAD PRO 12.9 (2018)

**From $1,529, apple.com/au**

The biggest iPad Pro is unbelievably powerful and slick, with an excellent screen, thin and compact design, great battery life and support for the Apple Pencil. Pricey, but worth it.

### APPLE IPAD PRO 11 (2018)

**From $1,449, apple.com/au**

Despite its smaller size, the internals of the 11in iPad Pro are the same as the bigger version: it's supremely powerful, it's incredibly versatile, in short, it's an absolute beast of a tablet.
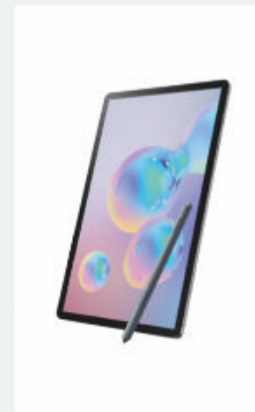
### APPLE IPAD AIR

**From $547, apple.com/au**

With a sharp, vibrant 10.5-inch screen, Apple Pencil support, mega-powerful A12 processor and thin, light body, this a Pro in all but name, for a bargain price. The best all-rounder tablet.

### SAMSUNG GALAXY TAB S6

**$999, samsung.com**

The finest Android tablet, this delivers a system with a sharp OLED screen, S Pen stylus, excellent audio credentials, powerful internals, and a neat laptop-aping DeX mode.

### NextMind Brain Dev Kit

US$399, next-mind.com
For anyone who already has their whole house connected via smart speakers, you'll know that having to ask AI to turn out all your lights or put on the heater gets tedious after a while. Thanks to NextMind Brain Dev Kit you no longer have to go through the effort of actually articulating what you want done, you can just think it and it happens. The wireless headset records neural activity in your visual cortex (presumably via magnetic field detection) and interprets the billions of neural signals into a command.



### Canon X Mark 1 wireless mouse

$55, canon.com.au
Computers are actually pretty good calculators and most OSes even come with some kind of calculator software baked into the launch package, but if you need the numbers and you need them now, then having a calculator directly on your mouse is even handier. Thanks to Canon there's a new wireless mouse in town that makes use of the space below the clickers and scroll wheel by filling it with an edge-to-edge calculator. Not only has this prime number managed to optimise space, but it doubles as an on-hand data entry pad for those using a tenkeyless keyboard.



# Gamer Bed Desk

You'll never want to get out of bed again.
$479, bauhutte.jp

If you are about to begin a fortnight-long self quarantine, then the Bauhutte gaming bed arrangement actually sounds like a pretty nifty setup. The Japanese company has designed this desk to attach to the end of your bed in order to "save you the difficulty of moving from your bed to your desk after you wake up". Along with an on-bed bean bag that sits you upright to see the screen, the desk can be accompanied by additional storage racks (for essential supplies like energy drinks and chips) and a gaming wear onesie that allows you to do away with the hassle of having more than one item of clothing.



# SubPack S2

This wearable subwoofer has your back.
US$299, shop.subpac.com

The SubPack S2 is the best '2' pack since Tupac, according to anyone who loves 'da phat bass'. With a frequency of 1 to 200Hz this dank doof duffel bag can be slung over your shoulders to pump thicc beats through your body. Weighing just 1.8kg and taking up no more than a hydration backpack, the SubPack S2 won't obscure the gun show and the soft shoulder pads allow you to slip it over your shredder singlet or go full shirtless if you're a Mr. Universe contender. Combine the S2 with the Razer Nari Ultimate face-bass headphones if you want to really shake things up. **TL**

# NBN SMB Solution for Ethernet WAN
## (FTTP, HFC, Fixed Wireless, Satellite)

**DrayTek** Aust & NZ
www.draytek.com.au

Ethernet WAN — NBN Ready

Ethernet WAN — UFB Ready
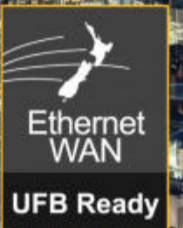
## Vigor2926 Series

**Dual-WAN broadband router with Gigabit LANs, SPI Firewall, 802.11ac (AC2000) Wi-Fi, VoIP and 50 x VPN tunnels including 25 x SSL-VPN**

**50x VPN**

- 1 x Gigabit Ethernet WAN port and 1 x configurable GbE WAN/LAN port for Failover and Load-Balancing and High Availability mode
- Two USB 2.0 ports for connection to two 3G/4G LTE USB mobiles, FTP server and network printer
- 4 x Gigabit LAN ports with multiple subnets and 50,000 NAT sessions
- 50 x VPN tunnels (including 25 x SSL-VPN tunnels) with comprehensive secure protocols
- Fast VPN throughput, VPN load-balancing and backup for site-to-site applications

Vigor2926Vac

- 16 x VLANs for secure and efficient workgroup management
- IPv6 & IPv4
- IEEE 802.11ac (AC2000) wireless Access Point; dual band; up to 1.7Gbps throughput (Vac/ ac model)
- 4G LTE SIM card slot (L model)
- VoIP with 2 x FXS and 1 x FXO Line Port (V model)
- Object-based SPI Firewall and CSM (Content Security Management) for network security
- Support VigorACS 2 Central Management System for remote network management
- Central VPN Management for 8 remote Vigor routers
- Central AP Management for deployment of multiple wireless VigorAPs
- Free Smart Monitor Network Traffic Analyzer for 30-nodes

## Vigor2915 Series

**Dual-WAN Gigabit broadband routers with 1 x GbE WAN, 1 x configurable GbE WAN/LAN port, 3 x GbE LAN ports, SPI Firewall, 802.11ac (AC1200) Wi-Fi, and 16 x VPN tunnels including 8 x SSL-VPN tunnels**

**16x VPN**

Vigor2915ac

- 1 x Gigabit Ethernet WAN port and 1 x configurable Gigabit Ethernet WAN/LAN port for Failover and Load-Balancing
- One USB port for 3G/4G LTE mobile broadband access, USB printer, storage and thermometer
- 3 x Gigabit LAN ports with 30,000 NAT sessions
- IPv6 & IPv4
- Object-based SPI Firewall, Content Security Management (CSM) and QoS
- 16 x VPN tunnels including 8 x SSL-VPN tunnels
- 802.11ac (AC1200) Wi-Fi, up to 300 + 867Mbps speed (ac model)
- Support VigorACS 2 Central Management System for remote network management
- 2 years back to base warranty

## Vigor2133 Series

**Broadband router with 4 x GbE LAN ports, SPI Firewall, 802.11ac (AC1200) Wi-Fi, VoIP and 2 x VPN tunnels including SSL-VPN**

**2x VPN**

Vigor2133Vac

- 1 x Gigabit Ethernet WAN port
- 2 x USB ports for 3G/4G access, FTP server and Network printers
- Load Balance and Failover functions for WAN and USB 3G/4G WAN
- 4 x Gigabit Ethernet LAN ports with 30,000 NAT sessions
- IPv6 & IPv4
- NAT throughput over 450Mbps
- Object-based SPI Firewall, Content Security Management (CSM) and QoS
- 2 x VPN tunnels including 2 x SSL-VPN
- 802.11ac (AC1200) Wi-Fi, up to 300 + 867Mbps speed
- SIP VoIP ( 2 x FXS) for Vac model
- Central AP Management for deployment of up to 2 wireless VigorAPs
- Support VigorACS 2 Central Management System for remote network management
- 2 years back to base warranty