PC MAGAZINE

FITNESS TRACKERS CHANGED MY LIFE

DIGITAL EDITION
MARCH 2018

PC MAGAZINE

CONTENTS

MARCH 2018

COVER STORY

FITNESS TRACKERS CHANGED MY LIFE

Just not in the way you'd expect

FEATURES

WHAT IS CYBER INSURANCE, AND DO YOU NEED IT?

Data breaches, identity theft, personal data theft... cyber insurance can cover that.

WHAT'S NEW NOW

FAST FORWARD

Lawrence Lessig on campaign corruption and the dangers of AI.

YOUTUBE'S COVERT CRYPTOCURRENCY-MINING ADS

A recent trend we're not particularly fond of.

PROTECTING YOUR BUSINESS FROM CRYPTOCURRENCY MALWARE ATTACKS

See above.

TOP GEAR

Intel Vaunt Smart Glasses, Petcube Bites, and Osmotex Hydro_Bot

REVIEWS

CONSUMER ELECTRONICS

Apple Homepod

Analogue Super Nt

DJI Mavic Pro Platinum

Panasonic Lumix DMC-FZ80

Apple Homepod

HARDWARE

Canon Pixma TS8120 Wireless Inkjet All-in-One

HP EliteOne 1000 All-in-One

HP EliteOne 1000 All-in-One

SOFTWARE & APPS

Online Personal Tax-Prep Services

NovaBackup PC

Analogue Super Nt

COMMENTARY

> **As far as I'm concerned, Bitcoin has no intrinsic value and should be worth nothing.**
>
> **JOHN C. DVORAK**
> Last Word

TIPS & HOW TOS

Our Quantified Selves

I've been reading Victoria Song's wearables reviews since she took over the beat last year. But it wasn't until she wrote this month's cover story that I appreciated the toll that tracking trackers could take on a human being. In her story, she shares the enthusiasms and disappointments of living a perpetually monitored life, where every trip to the watercool becomes a subject of quantification and analysis. That kind of mindfulness leaves a mark, and not just on your wrists. Wearables changed her life in some surprising ways, and there are some vital lessons in there for the rest of us.

First, the wearables revolution is moving a lot slower than we thought it would. Countless startups have folded, and even big players like Fitbit and Apple are struggling to make their products a daily habit. Battery life remains a real issue; and once someone takes off the device and misses a day, the incentives to put it back on start to fade. Who cares about steps, anyway? I've bought five different versions of the Fitbit—three of them were lost, and two sit in a dresser drawer, quite powerless.

At the same time, the power and impact of the data collected by wearables are going to be much greater than we imagined. Helping consumers lose weight and encouraging the deskbound to stand up once an hour is nice, but data can do so much more than that.

@dancosta

During the past year, 14,000 Apple Watch users have allowed a free app called Cardiogram to access their data. The company now claims its algorithms can detect diabetes with 85 percent accuracy. Furthermore, the company claims it can detect arrhythmia with 97 percent accuracy, hypertension with 82 percent accuracy, and sleep apnea with 90 percent accuracy. This is a remarkable step forward.

The ripples are already spreading through the healthcare industry. The economic impact is easy to see. More than 100 million US adults are diabetic or prediabetic. Treating them costs more than $266 billion a year.

And it raises an important question: Where does all of this data go?

Bear in mind that today's fitness trackers are not medical devices; they're just gadgets. That means they aren't regulated by the FDA, and perhaps more important, it means that HIPAA (the Health Insurance Portability and Accountability Act of 1996, which provides data privacy and security provisions for safeguarding medical information) doesn't cover the data they collect. So the only thing keeping your Fitbit, Apple Watch, or third-party app from sharing your personal data is the company's privacy policy. Have you read one of those lately? Neither have I.

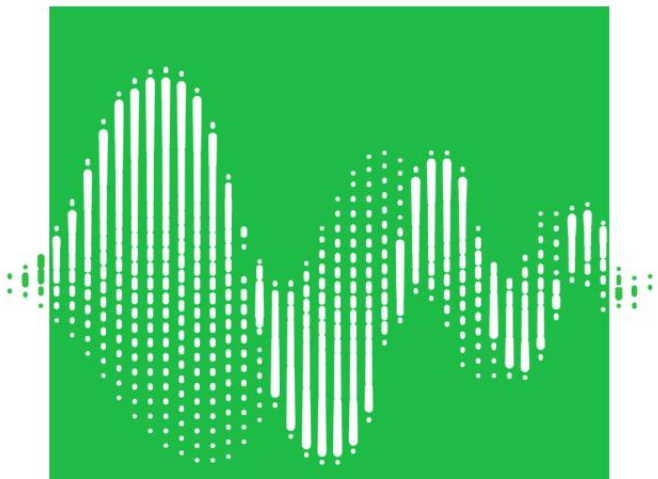
Victoria's story is filled with personal details she wanted to share with readers, but there's another record of all her wearables testing—a virtual log of steps, heart rates, and sleep patterns, as well as habits, medical conditions, and risk factors that, at

The power and impact of the data collected by wearables are going to be much greater than we imagined.

the moment, can legally be shared with anyone. United Healthcare already offers a plan that offers users $4 a day if they hit a certain fitness goals. What's to stop the company from imposing a penalty on its customers for missing those goals? And what employer would want to keep employees who are driving up its insurance costs? This is going to be a problem.

None of this will keep me from digging out my Fitbit Blaze, charging it up, and trying to get back into my workout routine next week. But as we focus on the healthy changes wearables can help us make, we should be aware of potential unhealthy consequences.

dan_costa@pcmag.com



Female Voice Assistants and Tech Addiction

In our February issue, a couple of opinion columns had commenters delving into the psychology behind the tech.

"THE REAL REASON VOICE ASSISTANTS ARE FEMALE (AND WHY IT MATTERS)"

Avoiding terms like she, her, foremothers, and the like can help remind readers that these are machines with audio interfaces. It's hard not to anthropomorphize them, though. And it is easy to assume the voices are female given the characteristics. (I wonder if the lead singers for bands such as Portugal the Man and Silversun Pickups have grown weary of being presumed to be female based on their voices.)

It may not be be an effective way, but avoiding such pronouns when referring to AI systems may help to avoid the transfer of bad behavior to humans that you are cautioning about. Such systems are always "it," never she nor he.
—reamon

I don't know. I think maybe [you're] reading too much into it. Before Siri and Alexa, we had two well-known examples of voice assistants. One was male, the other female. One actively tried to kill the users. The other was extremely helpful to users. You already know I'm talking about HAL 9000 from 2001 A Space Odyssey and Star Trek's USS Enterprise computer.

I would not discount the influence these had over those who create these assistants nor many who use them.
—Wesley Thaeron

I think that I am as concerned about women's status in our culture as a man can possibly be. I was surprised about the negativity in this article about using female voices for AI. If research shows that users find a female voice to be more "helpful, supportive, trustworthy" than a male voice, how does that reflect poorly on women?
—John A. Johnson

But there could be something else going on. A long time ago, when the military put voice warnings of imminent disasters into their aircraft ("Pull up, you a-hole—there is a mountain straight ahead!"), after much testing they chose a female voice. The explanation was that it would be listened to, cut through the clutter, and its meaning perceived more quickly than a male voice.
—John McGaw

I like choices, myself—I am a woman, and I prefer to hear a man's voice. Simple! Just give us all choices, and we will decide what we want to hear. Don't make the choice for me!
—frances20041

"TECHNOLOGY IS KILLING ME (AND PROBABLY YOU, TOO)"

Although I embrace technology as wholeheartedly as most... I also put the devices away when I get home from my IT job. Even my friends know they can't reach me by text after a certain hour, and that's the way it has to be. A long time ago, when I was still in school, my Cisco instructor warned me that I would get tired of technology if I didn't place limits on it. He was so right.
—maverick909

I am retired and stay at home and do not have a cellular telephone. My wife does and we drive with it. But she never uses it. AT&T loves her.
—Gary Masters

Ask us a question

Have a question about a story in *PC Magazine*, one of the products we cover, or how to better use a tech product you own? Email us at **letters@pcmag.com** and we'll respond to your question here. Questions may be edited slightly for content and clarity.

Fast Forward: Lawrence Lessig on Campaign Corruption and the Dangers of AI

Fast Forward is a series of conversations with tech leaders hosted by Dan Costa, PCMag's Editor-in-Chief. Lawrence Lessig is a professor of Law and Leadership at Harvard University, where we recorded the show. In 1999, he wrote Code and Other Laws of Cyberspace. Lessig is the cofounder of Creative Commons and made a run for president in 2016, which he sadly did not win. He's also the creator of the Lessig Method of Presentation.

Dan Costa: We're going to talk about the law, we're going to talk about the internet, we're going to talk about that messy place where the two collide. I want to start way back in 1999, when you wrote this book, and one of the things that you wrote in it is that "the code is the law." And you suggested that the internet will evolve into a more regulatable form. That was 18 years ago. Have we been moving in the right direction or the wrong direction?

Lawrence Lessig: Well, I think, unfortunately, I was right. I remember when I wrote the book, there was deep skepticism, because the argument of the book was the internet gives us lots of freedom right now, but that's only because of its architecture. And there will be lots of incentive both in business and in government, and business working with government, to change it into a much more regulable space. And that's in fact what's happened.

Whether it's just business, trying to make it easier to track and supervise what people do on the web to make it easier to sell them things, or business and government, where the government has worked with business to build back doors into software, or make it so that you can report more easily what's been happening. I think we've seen a pretty strong trend in the direction of regulatability.

And then some very interesting point of resistance. When Apple said they were going to encrypt by default, that was a really important step in the other direction. But strikingly, really the first by a major company to resist the increasing regulatbility of the net, and I think the fact that it's the first is what's really concerning me.

You also pointed out that there was going to be this trend toward consolidation. That there were a lot of forces that were going to drive this. At that point, it was wide open media. Nobody even really thought of it as a business platform; they thought of it as an open communications platform. But we have seen incredible consolidation in this space.

Yes, and it was actually something I wasn't thinking about at all, but it was so obvious in retrospect. It's just the fact that data is infinitely more valuable than even ownership of the platform and certainly ownership of the infrastructure. Because what data does is leverage all sorts of capability and potential for control and commerce. And the consolidation we've seen is that data induces a kind of winner-take-all dynamic for these platforms and you can't really afford to be number two, but if you are number one you are really, really incredibly successful. And I think nobody has a clear sense of how traditional principles of antitrust should apply in the context of this type of really dominant position that these companies play. And it's certainly too hard for me. I'm glad I'm far from this debate now.

Do you think there's anything unique about Facebook advertising and the micro targeting of individual consumers and playing on their fears, playing on their weaknesses, that platforms, like Facebook and even Google and Twitter, enable what just hasn't been there in the past?

Absolutely. I think the AI component to these machines is terrifying. You know, there's this great movie… called *[Colossus] The Forbin Project*… Dr. Forbin has invented a computer that's smart enough to run the defense of the United States. And so the president turns over to this computer control of the decision whether to launch nuclear weapons. Like, what could possibly go wrong?

At this point, it seems like that could be an improvement.

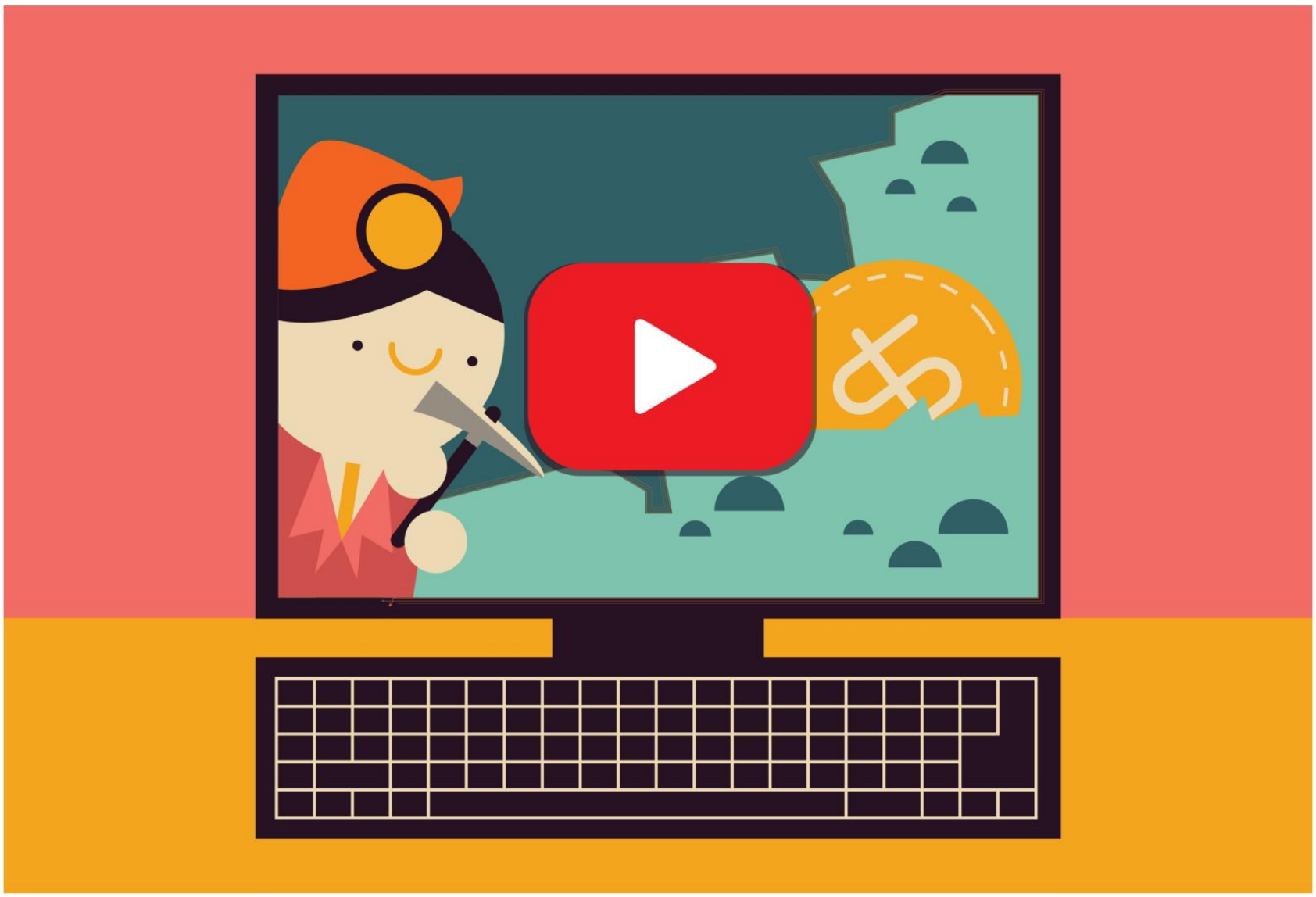
I'd take Dr. Forbin's computer over what we've got… That dynamic is people losing control of their technology. They don't understand where it's going to go. And there are really catastrophic consequences that can flow from that, and that's what I fear is happening in many different contexts here. When it turned out Facebook was selling ads to the category "Jew Haters," you know, there was no Facebook employee who created the category, "Jew Hater." This is generated by recognizing what the people in Facebook wanted in order to sell ads. And so it's a perfectly efficient technology for giving people what they want, but the fear is that dynamic can produce all sorts of ugliness that we don't actually want.

The data came out. I was on a panel with the CTO of Cambridge Analytica, who had been the CTO of the RNC, and he said, "Yeah, during the Trump campaign, we never let these things run on their own because we were afraid of where they would go." And you begin to get a sense of just how dangerous it is if even the Trump campaign was afraid of where it might go. And that's what keeps me up when I think about this dynamic. Because you're not going to turn off the incentive to become as efficient as you possibly can in delivering product to people on the commercial side. The danger is that that same dynamic when shifted to the democracy side, can produce all sorts of ugliness that I don't think we have a good way to think about solving.

See a video of the full interview and many more at pcmag.com/podcasts/fast-forward.

YouTube's Covert Cryptocurrency-Mining Ads

BY JOEL HRUSKA



Stealth cryptocurrency mining in one's browser without permission is one of our least-favorite trends of the past six months. The idea of end users generating income for the sites they visit by mining cryptocurrencies—as opposed to being hit with ads—has some interesting features to recommend it.

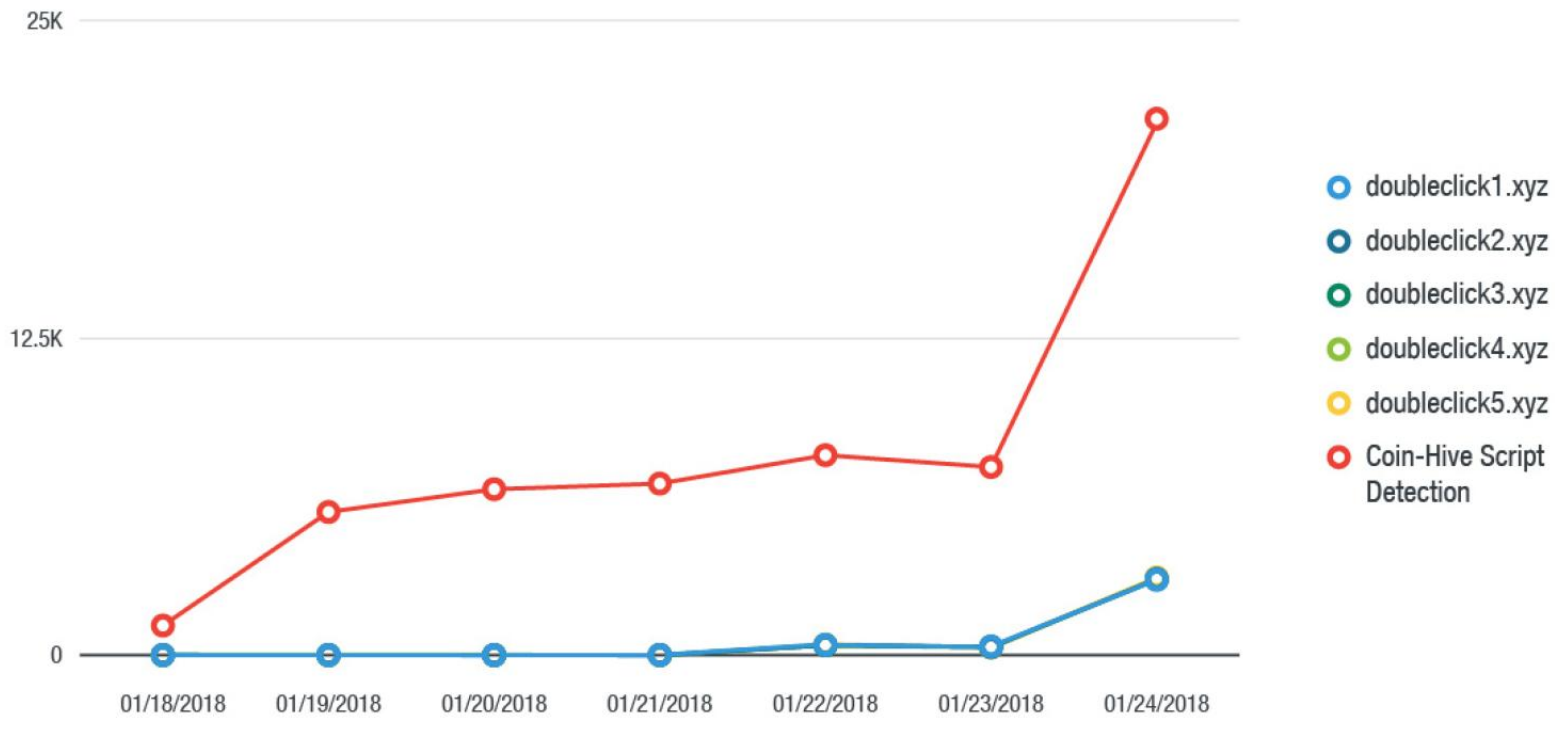
But it also raises some concerns and issues about how such funding should be monitored and controlled so that systems remain responsive—and to ensure that different sites and browsers won't slug it out for resources, with users left in the lurch.

Instead of an informed approach in which end users consent to such mining, we've seen stealth operations popping up everywhere: They steal CPU cycles from users, particularly if more than one crypto-mining program is running simultaneously (read this month's IT Watch story, "Protecting Your Business From Cryptocurrency Malware Attacks," for more). While most of these plugins are written to put just a light load on user's CPUs, that works only when the miner is running in a single browser instance, and only when it's running on a single site. Our tests in 2017 showed that using different browsers can defeat this dubious attempt to sandbox the performance impact. And, of course, even running one site still drains battery life more quickly than having the CPU properly idled.

"It's like someone figured out how to monetize the awful Flash ads everyone used to hate for eating CPU cycles."

It's like someone figured out how to monetize the awful Flash ads everyone used to hate for eating CPU cycles. A true win-win! And now, it's even hitting YouTube.

TrendMicro recently released an updated report showing a sharp rise in ads that were infested with cryptocurrency-mining software being served by Google's DoubleClick service:



Like other attacks, this one uses a Javascript miner to mine Monero via Coinhive. Here's how TrendMicro describes it: "The advertisement has a JavaScript code that generates a random number between variables 1 and 101. When it generates a variable above 10, it will call out coinhive.min.js to mine 80% of the CPU power, which is what happens nine out of ten times. For the other 10%, a private web miner will be launched. The two web miners were configured with throttle 0.2, which means the miners will use 80% of the CPU's resources for mining."

Earlier miners, just a few months ago, were sticking to much lower figures as part of a big to stay hidden. We were concerned at the time that this could escalate, and it looks as if it is. As more illicit services slug it out to steal this kind of processing time, your CPU's processing time is going to be a casualty.

If your system is running louder for no obvious reason, don't be afraid to pop open Task Manager and look for proof.

If your system is running louder for no obvious reason, don't be afraid to pop open Task Manager and look for proof. CPU utilization will be much higher if you've got a cryptocurrency miner stealing cycles.

Protecting Your Business From Cryptocurrency Malware Attacks

BY WAYNE RASH

Cryptocurrency may be the most notable success of blockchain technology, but not everything about it is gold. Miners have found a new way to make money for themselves while also reducing their costs. It's easy: They just have you pay for it.

What's happening is that hackers install code on a site that you're likely to visit for a long time. While you're there, an infected ad injects cryptocurrency-mining software into your computer, where it'll mine for currency while you're trying to do something else.

This practice appeared on YouTube in mid-January and was first reported by researchers at Trend Micro, who said that the DoubleClick ad network was being abused to deliver currency mining malware. The apparent reason was that people tend to stay on YouTube for an extended period, giving the currency mining software more time to work.

The malware comes from Coinhive, computer code that allows the mining software to run on other people's computers and use their resources. Reportedly, currency mining can suck up about 80 percent of a computer's resources, which leaves enough available that most people don't notice it during casual use.

THE BUSINESS COST

But your organization will notice, especially if the illicit cryptocurrency mining starts to spread on your network or especially on your servers. Even when you're paying for data center services, that computing power costs you money; if you lose capacity because unauthorized software is eating CPU cycles, then you may have to buy more capacity.

People tend to stay on YouTube for an extended period, giving the currency mining software more time to work.

It's also problematic when your servers or even your office computers get so bogged down that they can't deliver. Then you'll start have trouble operating key processes, which means you could lose business. While that 80 percent load might not be noticed on a consumer computer, you're probably not buying more computing power than you need for business use, so it's far more likely to be an issue. For example, during peak periods when your servers would normally run close to flat-out, they'll suddenly just be sort of flat.

During peak periods when your servers would normally run close to flat-out, they'll suddenly just be sort of flat.

Complicating the issue is that many of the hackers who use Coinhive distribute it from other people's servers as well. So if you're not protecting your public-facing servers, then a hacker could install it on your website. You could even inadvertently pass it along to your customers, who probably would not be thrilled to know they got it from you.

The most common way this malware makes it into servers is through vulnerabilities in Apache Struts or DotNetNuke, according to the folks at Trend Micro's TrendLabs. In case this sounds familiar, it was a Struts vulnerability that led to the breach at Equifax. Essentially, a hacker finds an unpatched website and installs the malware, which then transfers it to visitors.

PROTECT YOUR SYSTEMS

Fortunately, you can take action. The first thing to do is to patch your systems. The vulnerabilities in Struts and DotNetNuke have both been patched, but a lot of unpatched systems remain.

In addition, confirm that your servers and office computers have been patched. This may be more complicated than usual, with all the other patches related to the Intel vulnerabilities flying around. Nobody's exploiting those Intel problems, but they are using every exploit they find to make money with cryptocurrency mining.

It's worth noting that vulnerabilities that are being exploited for currency mining affect both Linux and Windows machines. So you'll need to patch all your servers, regardless of the operating system (OS).

Also make sure you have protection installed on all internet-connected endpoints, with updated anti-malware in place to keep the currency miners out. The way Trend Micro found the YouTube infestation was through a huge spike in blocking activity on that service and subsequent complaints. Trend Micro and other services, such as Malwarebytes, provide enterprise versions of their software for purposes such as this.

TRAIN YOUR STAFF

First, they need to know that if they get blocked from a website by your anti-malware package, then the solution is not to turn off the protection and hit the site anyway—it's to tell the security staff what they found.

Staff should also pay attention to unusual behavior on the computers they use, especially sudden bad performance. Cryptocurrency mining really loads down the CPU on a computer, and a sudden slowdown may be the first sign.

Finally, pay attention to your monitoring software. Typically, one of the parameters that these packages monitor is CPU load. So if yours spikes unexpectedly, currency mining might be the reason. Also bear in mind that those crypto-coins have to be uploaded somehow. If the computers on your network are mining, then it's your network that will be delivering.

“Staff should also pay attention to unusual behavior on the computers they use, especially sudden bad performance.”

Fortunately, crypto-jackers (as the illicit miners are called) rarely let their software deliver other malware such as ransomware. The reason? They want to use your computer as long as they can. After all, you're their cash cow, and they want to keep the milk coming.

What We Love Most This Month

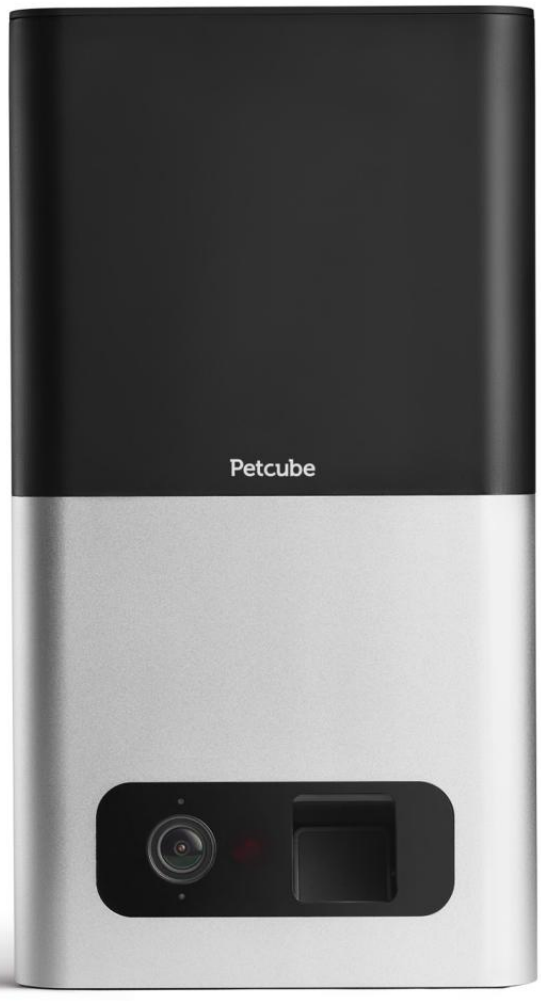
BY ANGELA MOSCARITOLO, CAROL MANGIS

Photo courtesy of The Verge

INTEL VAUNT SMART GLASSES

Smart eyeglasses have some handy use cases, but existing models are far from aesthetically pleasing. Intel is looking to bring some style to the world of smart specs. Although the Vaunt glasses look and feel ordinary (allowing wearers to skirt that Glasshole problem), they can project information such as directions and message notifications from your iOS or Android smartphone into your field of vision. The brains of the glasses live in the stems on the sides. Intel plans to launch an "early access program" for developers later this year.—*AM*

www.theverge.com



PETCUBE BITES

Watching your pets at home via webcam? That's nothing new—unless the camera can also reward them with treats. Petcube Bites is a 1080p streaming-video camera with a treat dispenser that you can control remotely, even specifying the distance that the treats are flung. Other features include night vision, sound and motion alerts, and two-way audio.—*CM*

$179.00; www.petcube.com

OSMOTEX HYDRO_BOT

Clothing fabric that wicks sweat away from the skin is a boon; no one enjoys that sticky, clammy feeling. Osmotex AG is taking wicking fabric from passive to active. Its Hydro_Bot technology lets textiles transfer moisture and vapor from the inside to the outside via battery-powered electroosmosis. It was created for use in extreme conditions such as mountain-climbing and challenging work environments, and the company claims the tech can match people's sweat rates in various climatic conditions and at different activity levels. Osmotex partner, KJUS, is expected to come out with Hydro_Bot jackets in time for ski season next winter. *—CM*

www. hydrobot.com

Chandra Steele

COMMENTARY

Bitcoin Is the New Beanie Babies

In the 90s, you had to take your entertainment where you could get it. Sometimes that place was the home shopping channel in the middle of the night. My brother and I would tune in to a fuzzy broadcast to watch a man in a cheap print shirt, who a short time ago had been selling knives, stand in front of a colossal rainbow mound of stuffed animals.

He'd pick up three or four in a fist, shake them at the television, and—in a coked-up sales pitch that left his mustache covered in spittle—yell things like, "You could pay for your kids' college tuition with these!"

That man was Don West, and he was selling Beanie Babies for hundreds of dollars. Of course, we now know that the former wrestling hype-man was not offering the most solid financial advice. Humphrey the Camel, once worth $2,000, can now be had for $15.99 on eBay. (Call now while supplies last!)

The current cryptocurrency frenzy is a modern-day corollary of Beanie Baby madness. Headlines about Bitcoin millionaires such as 19-year-old Erik Finman are reminiscent of stories about people like 9-year-old Cameron Johnson, who in 1994 was making $50,000 a year reselling Beanie Babies.

PCMag Senior Features Editor Chandra Steele got her tech journalism start at CMP/United Business Media. She also writes fiction and has been published in McSweeney's Internet Tendency.

Finman told Business Insider: “If you do not become a [Bitcoin] millionaire in the next 10 years, then it’s your own fault.” This surely makes some long for a heavy dose of karmic schadenfreude, but many have cryptocurrency FOMO and are making risky financial moves.

Students thinking about betting their college funds on Bitcoin should watch filmmaker Chris Robinson’s short documentary about his father’s obsession with Beanie Babies. He wanted to use his earnings to put Chris and his younger brother through school but ended up losing $100,000. Every pyramid scheme and lottery drawing features at least one person who makes it rich, but very rarely is that person you.

Early Bitcoin investor and millionaire Grant Sabatier, who runs Millenial Money, cautions against the high stakes of Bitcoin: It’s gambling, not investing, he says. That’s rare; in the cryptocurrency world, you’re more likely to encounter people like James Altucher. A self-described “crypto genius,” Altucher is one of the many people peddling cryptocurrency advice and schemes as though they were royal-blue Peanut the Elephants. While he makes his money from books, newsletters, and a podcast, he also pushes people into far less secure investments.

It’s important to separate cryptocurrencies and their underlying blockchain technology from disingenuous and overblown marketing. The value of Bitcoin and other cryptocurrencies is falling, but that volatility is one of the factors that can make this sort of marketing so enticing. Of course there will be those who say now is the time to go all-in. But that’s the same impulse that

fueled the purchase of armloads of soft stuffed toys in the 90s. Feverish economic groupthink can overtake good sense.

One of the latest ways to peddle cryptocurrency is through an initial coin offering (ICO), which is much like an IPO but without any regulatory oversight (for now). A startup raises funds by accepting Bitcoin or other cryptocurrencies to get itself off the ground, in rapid sales that can last hours or even minutes. Facebook is not known for taking swift action against advertisers or others on its site, but there have been so many ICO scams that the social network's cryptocurrency ad ban was a no-brainer.

Beanie Babies might be gone, but their spirit lives on in Bitcoin. Where there once was Don West on a UHF channel, there's now boxer Floyd "Money" Mayweather on Instagram. When you look at those stacks and stacks of cash Floyd is about to invest in an ICO for Stox.com, know that it's throwing good money after bad.

"Altucher is one of the people peddling cryptocurrency schemes as though they were royal-blue Peanut the Elephants."

Sascha Segan

COMMENTARY

Don't Be Afraid of Huawei and ZTE

Don't throw out your ZTE phone. US intelligence chiefs paint a dark picture of ZTE and Huawei, which they claim are Chinese spying operations, but we haven't seen a shred of actual evidence that either company's phones are dangerous to Americans in any way.

Sascha Segan is the lead mobile analyst for *PC Magazine*. His commentary has also appeared on Fox News, CNBC, CNN, and various radio stations and newspapers around the world.

The bigwigs' most recent admonition is part of a long campaign against ZTE and Huawei, started by Congress in 2012. At that time, Huawei pretty much backed out of the US market, but ZTE doubled down, started sponsoring the Houston Rockets, and became the number-four smartphone seller in the US.

The change we need to talk about is that the officials have switched from blocking Huawei network equipment to disparaging Huawei and ZTE handsets. Both companies have been essentially banned from our network equipment market for five years now, and no US wireless provider uses their products.

Network equipment is, in general, where spying happens. You can dragnet a lot of communications at once, it's jealously guarded by wireless carriers, and independent researchers often don't have access to it. You don't even have to have special backdoors in the network

equipment to spy. The SS7 network flaw is widely thought to be used by intelligence agencies around the world to spy on cellular traffic.

When the UK and Australia have criticized and blocked Huawei in the past, it's always been about network equipment. Australia banned Huawei network equipment from its national broadband network and then issued both Huawei and ZTE phones to government staff members, demonstrating the huge difference between how network equipment and phones are seen.

Note that US intelligence chiefs also don't say there's a specific threat. Rather, they just don't like these companies, because China. There's no actual evidence. Just... China.

"We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks," FBI Director Chris Wray testified, as quoted by CNBC.

That is not "these phones are an actual threat." That is "I just don't like these companies." Huawei and ZTE, obviously, say that they are not security threats, they're committed to openness and transparency, and whatever.

HANDSETS ARE DIFFERENT

Network equipment is used by a relatively small number of large corporations, which guard their secrets tightly. It isn't widely, aggressively, and publicly tested by a large security researcher community.

But handsets are tested by everyone. As soon as a new phone comes out, everyone from global security research firms to random geniuses on XDA-developers start disassembling the firmware; iFixit and other teardown firms take electron microscopes to these things.

This crowdsourced research has turned up problems in handsets, including Chinese handsets, again and again. Both OnePlus and Blu have been caught delivering security flaws to their customers. They were both roundly roasted for their errors, and changed their ways.

Nobody has ever found this supposed spy software inside Huawei and ZTE handsets. The people asserting that it may exist have never described it and never identified specific models that include it. The US also stands alone in essentially blocking Huawei's phones, rather than network equipment.

To believe this software exists, you'd have to believe that Huawei and ZTE are so far beyond the capabilities of any other manufacturer that they're able to hide this tech when others cannot. You'd also have to believe that we've found an exploit that CSIS, MI6, and the Mossad have all missed, and that we haven't shared it with any of our allies.

If you're worried about being surveilled, I have bad news for you: You are being surveilled. Your wireless carrier has mountains of data on you, and will turn it over to the government at the drop of a warrant. Google and Facebook have terrifyingly accurate profiles of what you do, what you think, and where you are. All those organizations have reason to be interested in you. They want to sell you ads or make sure you obey their laws and rules.

Even if Huawei and ZTE were spy operations, and I don't think they are, they don't have urgent enough motivation to risk massive, global shame and business collapse by installing spyware on tens of millions of phones willy-nilly. The Chinese government has no motivation to be spying on you, specifically. Unlike the Australian defense staff who use ZTE phones, you do not have any information that any foreign government actually wants.

I know it may hurt to know you're not important. "But no!" you cry. "I have critical trade secret information the Chinese must want to steal!" You don't. They don't care enough to steal it. Unless you actually work for the government or military, in which case you should be using a product that's on the DoD recommended list, you are not being caught in any sort of Communist dragnet. Paranoia will destroy ya.

OUR VERDICT: WE AREN'T BOTHERED

Years of Huawei and ZTE phones being in global markets, being explored, examined, downloaded, disassembled, recompiled and hacked upon have revealed no more critical security flaws than in any other Android vendor, and they haven't shown that the handsets are spying for the Chinese government.

The intelligence officials disparaging these companies have also given no evidence and been careful not to state that the handsets themselves are a clear and present threat—just that they have an animus against these companies.

Without any actual evidence of wrongdoing, we have no problem recommending Huawei and ZTE phones to buyers in the US, and you shouldn't have any concerns buying them.

sascha_segan@pcmag.com

Max Eddy

COMMENTARY

The Shifting State of Android Security

In a recent blog post, Google outlined some Play Store security stats, an unusual move for the company that signals a larger shift within Google. The post—from Dave Kleidermacher, Head of Security, and Andrew Ahn, Google Play Product Manager—portrays Google as an active guardian. In 2017, it took down 700,000 apps that violated Google Play's policies, a 70 percent increase in removals over the year before, it said.

PC Magazine Software Analyst Max Eddy has also written for publications such as _International Digital Times_, _International Science Times_, and _The Mary Sue_.

I've written about Android security for several years now, and I can say it's disappointing to see how fast low-quality and even malicious apps can spread through the Play Store. It hasn't been unusual for me to get tipped off to a malicious or at least unsafe app—and see that thousands of people had already downloaded it. But Google says 99 percent of apps with what it calls "abusive content" are now snagged before they're published.

"This was possible through significant improvements in our ability to detect abusive app content and behaviors—such as impersonation, inappropriate content, or malware—through new machine learning models and techniques," Kleidermacher and Ahn wrote.

@wmaxeddy

Google labels the really bad stuff—apps that can secretly send, receive, and intercept SMS messages for nefarious activities—as Potentially Hazardous Apps (PHAs). They act as Trojans, or they phish victims for personal information to send back to the bad guys. In short, these apps are designed to do actual harm.

Here, Google is less specific about improvements. "While small in volume, PHAs pose a threat to Android users and we invest heavily in keeping them out of the Play Store," Kleidermacher and Ahn wrote in their post. "With the launch of Google Play Protect in 2017, we've reduced the rate of PHA installs by an order of magnitude compared to 2016."

But Google is not just targeting apps. In 2017, it revoked the privileges of 100,000 so-called "bad developers" who filled the Play Store with the chaff that has plagued it for years. Google says it's now more difficult for these bad actors to create new accounts and simply republish their apps—a great step toward cleaning up the Play Store.

Not all "bad" Play Store apps are malicious. Most are merely misleading and low-quality, impersonating more popular apps from mainstream developers and making money with aggressive advertisements. Google says it took down over 250,000 apps that impersonated a different app in 2017.

A popular (but dubiously accurate) critique of the Play Store is that it has relied too heavily on automation to approve apps. Google, for its part, has told me that humans were always involved at some level of its app approval process.

We've seen glimpses of this before. At the 2017 Google I/O conference, the company said 20,000 dedicated processors reviewed 500,000 apps a day for potential malware. The influence of machine learning and associated AI technology has only increased. A Google rep told me that the Play team is applying machine learning more broadly, to identify not just bad apps but also the developer networks that create them.

Machine vision, the rep continued, is also improving the Google Play experience. The system can identify bad apps more accurately and do so at scale. "We have much more data than before for the models to train on so they can better detect nuances and hidden abuse," the Google rep said. "And [machine learning] has helped make human reviewers be more effective."

This is all part of a larger shift I've seen in how Google handles Android. In the past, I'd always felt Android put hardware and software developers' interests ahead of consumers. For example, it took years for Google to implement an Apple-style permissions model, where users could approve or reject specific permissions for each app. Previously, Android required you to accept whatever the app requested if you wanted to use it. And in Android 8.0 Oreo, stricter limitations on what apps can do in the background are intended to give users a better experience.

"The initial focus/priority for Google Play/Android was to enable developers [to] reach a big global audience and bring fast adoption of the platform," a Google representative told me. "Now that Google Play has reached critical mass, we've definitely shifted gears to focus on building a trusted and safe store. We want to make sure users get a high-quality experience."

That's a change of tune I'm glad to hear, and one that I hope continues.

max_eddy@pcmag.com

Apple HomePod

$349.00

●●●◐○

Apple HomePod Sounds Great but Is Shortsighted

The Apple HomePod is a high-quality smart speaker for your Apple Music account and iTunes library, with some Siri voice assistant features that help especially with smart home usage. The hardware is excellent, but right now, Apple doesn't have the broad vision for voice-assisted living that the Amazon Alexa and Google Assistant platforms show.

Looking at voice platforms as the next world of computing, the HomePod seems very lonely. Alexa and Google Assistant are systems, and they become more powerful as they spread through your house. Your living room Google Home Max is complemented by your kitchen Home Mini, which you use to broadcast, "It's dinnertime," to the kids' rooms. Your bedside Amazon Echo Spot wakes you up to music, and then you tell the Echo Dot in the foyer to turn off the lights when you head out on your commute.

The HomePod is priced, sized, and skilled to be a living-room music speaker for other Apple devices. In that context, the HomePod comes off as more like the Apple Watch or the Apple TV: not a new, core product category but an accessory to enhance your iPhone ownership and make sure you keep paying that Apple Music subscription fee. Since other voice-assisted speakers can't play Apple Music, the HomePod is the obvious choice for iPhone owners and Apple Music subscribers who don't want to pay an extra tithe to Amazon, Google, or Spotify.

From an audio standpoint, the HomePod delivers a rich, balanced sound signature that highlights the mids and highs. It doesn't distort at top volumes, and its bass depth is impressive for its size. The HomePod's sound can fill a room, but it doesn't get quite as loud or deliver quite as much deep-bass response as the slightly pricier Google Home Max.

Apple HomePod

PROS Powerful audio performance with rich, full bass. Measurement mic adjusts audio according to your room's acoustics. Visually pleasing design.

CONS No Bluetooth streaming. No aux input. No way to disable DSP. No voice control for non-Apple music services. Siri is behind the competition.

And we can't recommend it as a broad solution—at least not yet—for people who are considering diving more deeply into home voice assistants. The HomePod plays music. It sounds great. It controls your smart lights. But unlike Alexa and Google Assistant, it doesn't yet have the ambitions for more.

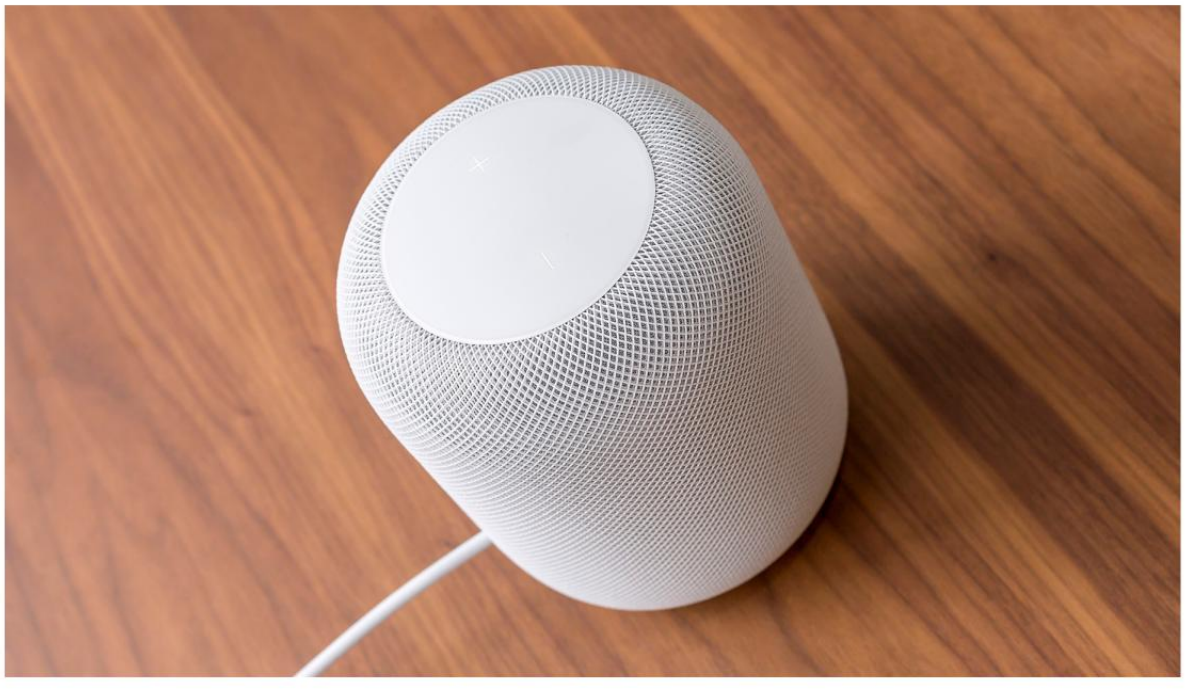
DESIGN AND SETUP

The HomePod is smaller than you might think and covered in a mesh fabric, except for the glossy, touch-sensitive top panel. It's 6.8 inches high and 5.6 inches wide and weighs 5.5 pounds. Sitting alongside the Google Home Max, the HomePod looks rather small; it's slightly larger and wider than the Sonos One. Regardless of size, all three speakers look like they come from the same Black Mirror prop shop, which is actually an across-the-board compliment.

The only visible controls are volume buttons on top. Tapping the panel in various patterns also works to control play/pause, fast forward, and rewind. An animated LED waveform appears on top when you speak to Siri—this signifies that Siri is listening to you. There's no mic mute button, but you can say, "Hey Siri, stop listening," to turn off the mic and tap on the top when you want to turn it back on.

Apple's commitment to portless elegance goes too far, in our view. The HomePod has no aux input for wired playback. In fact, there's not a single connection on the speaker. Even the power cable is hardwired, so if it goes bad down the road, you'll have to send the whole speaker in for servicing rather than just get a new cable. 9to5Mac says, after seeing an internal Apple memo, that a cable replacement costs $29.

From an audio standpoint, the HomePod delivers a rich, balanced sound signature.



The HomePod is a small but powerful speaker designed to be used with Apple's phones and tablets.

Internally, the speaker uses an array of seven tweeters firing in all directions, each one individually amplified, and an upward-firing woofer with its own amplification. The product's specs list all sort of exotic features ("internal low-frequency calibration microphone for automatic bass correction," "transparent studio-level dynamic processing") that basically add up to the same thing: The HomePod uses digital signal processing (DSP) to alter its audio output.

Mostly, this means the speaker limits dynamics and bass response when it's blasting at high volumes, primarily to prevent distortion. It's the established norm with wireless speakers in this price range and lower.

Like some soundbars and home theater systems we've tested, the HomePod also measures the room it's in and adjusts the audio according to its acoustics—that's what that calibration mic is for. All of this, as well as the streaming and buffering of audio, is powered internally by the Apple A8 chip. The mics are sensitive and had no problem hearing us say "Hey Siri" over loud music.

To set up the HomePod, you'll need an Apple iPhone 5s or later, an iPad Air or later, an iPad mini 2 or later, or an iPod touch. You can't set it up without an iOS device, even with a Mac. You also need a Wi-Fi network; it won't run without Wi-Fi.

Setup is dead simple—easier than with Amazon or Google and far easier than Sonos. Just wave your phone near the speaker, and it'll borrow your phone's settings and get going.

PLAYING AT HOME

The HomePod is designed to be used with an Apple Music subscription. Without a subscription, it can play Beats 1 radio, music you bought from Apple, podcasts in Apple's library, or anything via AirPlay. If you have an iTunes Match subscription but not Apple Music, it can also play the uploaded or matched music in your iCloud Music Library. It does not have Bluetooth or a 3.5mm input. (The speaker itself has Bluetooth but uses it only for pairing.)

Technically, the HomePod supports HE-AAC, AAC, MP3, Apple Lossless, AIFF, WAV, and FLAC music. But all those formats are processed through AirPlay or Apple's cloud.

Audiophiles should remember that when you play your synced music through the cloud from your iCloud library, it will play at 256kbps AAC. AirPlay is 44.1kHz lossless streaming, though, and you can AirPlay any file that iTunes can play. We even AirPlayed from a Windows PC without a problem. If you play from an Android device, though, you'll struggle; third-party AirPlay apps for Android are unreliable and fall in and out of compatibility.

The glowing light on top tells you Siri is listening. You can tell Siri not to listen, if you want to temporarily disable the mic.

The speaker won't work in tandem with others or as part of a multi-room set—yet. Apple says later this year, it will offer the option to pair two HomePods for stereo sound (the way Google allows with its Google Home Max), and to use AirPlay 2 to create multi-room sound stages.

Unlike other voice assistant speakers, the HomePod lets you request songs from Apple only by voice—not from Spotify or other radio services. But you can AirPlay other streaming services from your iPhone or computer. We tried Google Play Music, Pandora, Spotify, and YouTube Music, all on an iPhone X. They all let you say things like, "Next track," to skip a track, pause and resume songs, and ask the name of a song. But they had a few bugs. YouTube Music would sometimes start in the middle of a song when I said, "Next track," and Pandora had a noticeable delay in fast forwarding.

AUDIO PERFORMANCE

On tracks with intense sub-bass content, like The Knife's "Silent Shout," the HomePod delivers a powerful bass thump that is impressive for its size. At maximum volume, the bass doesn't distort, and the speaker gets quite loud, though it's not as loud or powerful as the Google Home Max. The Home Max is able to provide more palpable subwoofer-like depth, but the HomePod sounds more mids- and highs-focused while still delivering some rich, full bass response. At moderate volumes, the bass response is often stronger, as it's less affected by DSP.

Bass response is one area where the calibration mic probably helps. Where you place a speaker—how close it is to a wall, the vibrations of the surface it's placed on—can really impact bass levels, sometimes in a positive way but most often not. The HomePod aims to regulate this variable and provide you with consistent bass depth, so that what you hear when you place it in the corner shouldn't vary wildly from what you hear when you place it in the middle of a room. Theoretically, this is great, but having no control over it at all is bound to drive some audio lovers insane.

Bill Callahan's "Drover," a track with far less deep bass in the mix, gives us a better sense of the HomePod's overall sound signature. The drums on this track can sound overly thunderous on systems that heavily boost the bass, but through the HomePod, the drums sound more modest—not at all thin but not as heavy as some bass-centric speakers make them. The more obvious bass depth is instead found in Callahan's baritone vocals, which sound especially full and rich here.

The HomePod autocalibrates using its microphones, tweeters, and A8 chip, to provide good audio performance wherever you place it.

This would make the HomePod's sound signature muddy were it not for an excellent high-mid and high frequency presence that adds some treble edge to the vocals and lends some additional brightness to the guitar strums and extra snap to the higher register percussive hits. This is a balanced, rich sound signature—Apple's DSP may not be transparent, but it honors the basic intentions of the mix and doesn't exaggerate low frequencies or add too much sibilance or brightness.

On Jay-Z and Kanye West's "No Church in the Wild," the kick drum loop receives the ideal amount of high-mid presence, allowing the loop's attack to retain its punchiness and push through the layers of the mix. The loop also gets some pleasant lower-frequency depth added in, nothing too intense and mostly in the lows and low-mids. The sub-bass synth hits that punctuate the beat are delivered with solid presence, but especially at higher volumes, we get less deep sub-bass from them and hear more of their raspy top notes. In other words, the DSP kicks in and limits the bass response in the sub-bass frequencies.

At moderate volumes, the DSP does less of this, and so the bass can actually sound more full and deep than when you crank things up. The vocals on this track sound crisp and clear and never veer into overly sibilant territory. Generally speaking, vocals sound great through the HomePod across the board. The DSP does a fine job of prioritizing high-mids and highs, and this results in a crisp delivery.

For orchestral tracks, such as the opening scene from John Adams' *The Gospel According to the Other Mary,* the lower-register instrumentation gets a modest amount of boosting, but the stage still belongs to the higher-register brass, strings, and vocals. This is one genre that seems to sound less adjusted by the DSP than others—there's little in the way of sub-bass, but when it appears in the mix, its presence is modest. The lower register strings on other classical tracks have a lovely rich quality to them, and things generally sound quite natural on orchestral tracks across the board.

The lower register strings on other classical tracks have a lovely rich quality to them.

Playing these tracks via Apple Music versus streaming them, say, from a phone with AirPlay, the difference in audio performance is almost too subtle to mention. When you're playing high-res lossless files over AirPlay (from an iOS device or Apple computer), you're technically listening to a higher quality stream than when listening to Apple Music, but remember: It all goes through the DSP, and the DSP can't be disabled.

Thus the concept of "lossless" as far as the HomePod is concerned must be married to the concept of a somewhat sculpted sound signature—even when your source file is pure as can be, it will be subject to Apple's sonic sculpting. This is a negative for purists, but plenty of listeners will find the overall audio performance and DSP to be quite favorable.

The only visible controls on the HomePod are the volume buttons on the top, but tapping the top in various patterns controls play/pause, fast forward, and rewind.

The HomePod has one woofer and seven tweeters, all tucked under a fabric cover that comes in gray or white. The cover is not removable.

GET SIRIOUS

The HomePod uses Apple's Siri as its voice assistant, although its version of Siri isn't as powerful as the one in your phone. It's very, very focused on what Apple thinks you should be doing with it, which is playing music and controlling your smart home.

According to a report from IFTTT, most people use smart speakers to stream music, control lighting, set timers, and get the weather. The HomePod does fine with three out of those four tasks; it's just lousy with timers.

But that makes sense, at least, considering the HomePod's size and cost. It's designed to be a music speaker at the focus of your living room. It's not supposed to be a bedside alarm clock, unlike the Amazon Echo Spot, or a kitchen timer, or a multi-room intercom system as Echo Dots and Google Home Minis are.

MUSIC QUERIES

I came up with 25 queries to ask the HomePod, Amazon Echo, and Google Home, to check out the difference between the systems.

All three speakers had no problem playing songs by name. When asked to "play 80s new wave music" or "play old-school hip-hop," all the speakers came up with custom playlists that worked with the genre. Fair enough.

Things got a little odd when I asked the speakers to "play something upbeat," "play something sleepy," and "play some quiet music." For upbeat, Alexa picked a pop playlist, Google picked jazz, and Siri picked funk. For quiet, Alexa gave me Ed Sheeran, Google chose a Janet Jackson ballad, and Siri went with Steely Dan. And for sleepy, Alexa delivered nature sounds, Google had some relaxing electronica, and Siri gave up and played Wiz Khalifa.

Finally, I asked the speakers to "play something I'd like." Alexa and Google gave up there, trying to find songs by that title. Siri got the intent right but launched into an emo track by Rise Against, which I do not like.

HOME AND KITCHEN

HomeKit is one of the HomePod's great strengths. You can now control by voice any smart devices and systems you've set up through your iPhone, including scenes and zones. We easily turned lights on and off using the HomePod, even with our iPhone turned off.

The HomePod falls short as a timer because it can set only one at a time. You can get around that by setting alarms for specific times of day (for instance, ask Siri what time it is, and then set an alarm for three minutes later), but Amazon and Google both support multiple named timers, which is much smoother.

Siri falls flat on recipes, too. Alexa and Google both read out a range of recipes and ingredients, step by step. Siri just says, "I can't get the answer to this on HomePod." Don't use it in your kitchen.

NEWS AND GENERAL KNOWLEDGE

Here's where Siri really starts to fail.

The HomePod gets its weather data from weather.com. All three voice systems responded to, "What will the weather be tomorrow?," "Will it rain tomorrow?," "Do I need a coat?," and "Do I need an umbrella?"

In terms of news, the HomePod is more limited than the competition. It'll play you a news brief from CNN, Fox News, NPR, or the *Washington Post*. Both Alexa and Google have hundreds or thousands of news sources.

When you ask for calendar events, Siri says, "I can't access your calendar here." Alexa has various calendar skills; Google tells you your Google calendar events as long as you don't have a G Suite account.

As for general knowledge queries, which we're lukewarm on testing anyway because they feel gimmicky, Google did much better than either Alexa or Siri, spelling the world "querulous" correctly (the other two misunderstood what I was saying) and telling me how many albums Belle and Sebastian made.

Siri also falls way short when it comes to third-party branded skills. Alexa and Google can order you an Uber, for instance, buy you movie tickets, and plug into third-party notes and to-do services. Siri, at least for now, can't do any of these things.

It really isn't clear how many third-party services plug into Siri; Apple wouldn't give us a list. But it's certainly many fewer than the 2,000 skills for Google Assistant, or the 24,000 for Alexa.

OTHER COMPARISONS

The Echo and Google Home devices can make outbound phone calls; the HomePod cannot, although it can be used as a speakerphone for an existing call on your iPhone. All three devices can send texts.

> **The Amazon Echo and Google Home devices can make outbound phone calls; the HomePod cannot.**

The HomePod can connect to only one Apple account, and it doesn't verify voices. (Google Home can automatically respond to up to six different people using their accounts, and Alexa can be asked to switch accounts.) That means when you hook up SMS messaging, anyone will be able to send texts from your phone number through your HomePod, as long as your phone is in range.

Also, unless you tell the HomePod to “turn off use listening history,” everyone’s music selections will be taken into account when you ask for custom playlists, which could add up to some odd results. Alexa and Google Home are much better at balancing the needs of families.

CONCLUSIONS

The HomePod is a sonic success. Purists may thumb their noses at the DSP and overall inability to disable the room-adapting technology in favor of an unadulterated signal, but we can confirm that although the audio performance may be steeped in digital processing, it almost always sounds rich, full, and clear. The speaker is easy to set up and effortless to use, as long as you’re playing Apple Music.

But while the HomePod makes a great living-room speaker for your Apple Music subscription, it’s neither the core of a voice-activated home nor the best smart speaker available. Our Editor’s Choice for high-end smart speakers, the Google Home Max, is larger and more powerful with better volume, better bass depth, a better voice assistant, and more flexibility with music services and inputs. The Home Max can also become part of a household system with various smaller Google Assistant speakers. Apple doesn’t have such a range available. For now, the HomePod stands alone.

We’re also irritated at how the HomePod doesn’t play well with others. The lack of Bluetooth input, aux input, and support for more music services feels to us more like a marketing move to lock you out of non-Apple music sources than a consumer-friendly, quality-oriented choice.

The HomePod feels unfinished, but we wouldn’t count Apple out. The first iPhone felt unfinished, too, with its poor-quality phone calls, lack of 3G, and lack of apps. The first iPod didn’t support Windows. The HomePod is an admirable first try. It’s entering a realm where the competition has been working on its products for years. Let’s see how fast Apple can catch up.

SASCHA SEGAN, TIM GIDEON

Analogue Super Nt: Superlative Retro Gaming

PC MAGAZINE EDITORS' CHOICE

Calling Analogue a niche retro gaming company undersells what it does. The company's first product, the Analogue Nt, was a game system that could play Nintendo Entertainment System games and output them at 1080p over HDMI. It also had a solid metal body and cost $500. The Super Nt isn't metal, but it has a much more reasonable price and offers the best emulation-free SNES/Super Famicom gaming and 1080p upconversion you can get. This system is for a very specific type of retro game collector, for whom it undoubtedly earns our Editors' Choice.

Analogue Super Nt
$189.99
●●●●○

DESIGN

Although the Super Nt doesn't have the solid aluminum body of the Analogue Nt or Mini Nt, it's still a hefty little device. At 1.6 by 6.5 by 5.2 inches (HWD) and 17.6 ounces, it's almost twice the size of the SNES Classic and over three times its weight. The Retro-Bit Super RetroTrio Plus and Hyperkin RetroN 5 weigh 21.9 and 31.4 ounces, but they're also about two and three times larger than the Super Nt. Analogue wins the battle of the retro game consoles in terms of sheer density.

Analogue Super Nt

PROS Immaculate upscaling. Flexible graphics options. Supports legacy controllers. Excellent build quality.

CONS Expensive. Doesn't include a controller.

The Super Nt has a cartridge slot on the top panel, with power and reset buttons underneath.

It isn't a nearly perfect miniaturized version of a Super NES, like the SNES Classic is, but the Super Nt has an attractive design with classic notes that retro game fans will appreciate. Its slightly curved box shape hails back to the Super Famicom, the original Japanese version of the SNES that featured a much sleeker design than its more angular American counterpart. The similarities are even more apparent in the SF version with its light- and dark-gray color scheme based on the Super Famicom. The Super Nt is also available in Classic (SNES-style light-gray with purple buttons), Black, and Transparent models.

Like the original systems, the Super Nt has a cartridge slot on the top panel, power and reset buttons under it. They're pushbuttons, like those on the Super Famicom, rather than sliding switches like the ones on the SNES. The Super Nt has no mechanical eject button; you remove cartridges simply by pulling carefully as you hold the system in place.

The back of the Super Nt has only a micro USB port for power through the included wall adapter and an HDMI port for hooking the system up to your TV. Since most of the appeal of the Super Nt is its excellent upscaling, it has no legacy video outputs for connecting it to a standard-definition TV. An SD card slot on the right side of the system lets you update the Super Nt's firmware, should Analogue releases a new version.

"The Super Nt has an attractive design with classic notes that retro game fans will appreciate."

CONTROLLERS

Two SNES/Super Famicom controller ports sit on the front of the Super Nt. Analogue doesn't include any controllers with the system, which is a shame considering its fairly steep price. But you can order the 8Bitdo SN30 gamepad and SNES Retro Receiver through Analogue, along with the Super Nt, for $40.

The SN30 is a Bluetooth version of the 8bitdo SN30 2.4G we reviewed for use with the SNES Classic. It's an impressively accurate recreation of the original SNES and Super Famicom gamepads that feels excellent and works completely wirelessly thanks to the Retro Receiver that fits into either controller port. Since the Super Nt uses the original SNES/SF controller port, you can also use original SNES gamepads or any number of third-party reproductions.

INTERFACE

When you turn the Super Nt on, the system takes a few seconds to boot up and then brings you to a main menu, where you can access whatever game is inserted in the cartridge slot, change settings, or play Super Turrican Director's Cut or Super Turrican 2 (the only two games built in). Since the Super Nt uses SNES hardware and cartridges rather than emulation to play its games, the presence of two clearly digital games on the system is a bit strange.

Super Turrican was originally released on the SNES in 1993. It was developed by Factor 5, which made Turrican and Turrican II for the Amiga and Atari ST and Mega Turrican for the Sega Genesis. The finished version of Super Turrican was 6MB, which had to be cut down to release the game on a 4MB cartridge. Super Turrican Director's Cut is the original version of Super Turrican, restoring all of the dropped content. Because the uncut version of Super Turrican was never released and not put on any of Nintendo's Virtual Consoles, its presence on the Super Nt is a rare opportunity to play the full game as developed. Super Turrican 2 is simply a nice bonus.

The options menu shows you how much effort was put in the Super Nt's video processing. To start with, you can set the Super Nt to output video at 480p, 720p, or 1080p at 50 or 60 frames per second. You can also choose from a variety of upscaler filters that provide different smoothing effects. I greatly prefer the No Upscaler option, which simply blows up each pixel, reproducing it crisply to show off each game's sprite art without any attempt to round out sharp edges. You can also toggle scanlines for a CRT effect and even adjust the shape and density of them.

By default, the Super Nt goes through a startup animation that lasts several seconds before opening the main menu. It's tedious after you've seen it a few times, but fortunately, you can simply set the console to automatically boot into whatever cartridge is inserted, bypassing the animation.

CARTRIDGE COMPATIBILITY

Besides the two Super Turrican games, the Super Nt relies entirely on your own SNES and Super Famicom game collection. So you'll need cartridges, if you don't already have them. And those cartridges have to be in good condition.

If you haven't played the games in a while, clean the contacts using cotton swabs and isopropyl alcohol. A set of Gamebit screwdrivers lets you open up the cartridges to clean the full length of the contacts and to make sure that none of the components on the inside are broken. Several of my games didn't work on the Super Nt until I gave them a thorough cleaning. After that, they played flawlessly.

The Super Nt doesn't use emulation, as the SNES Classic, Hyperkin RetroN 5, and Retro-Bit Super Retro-Cade do. Instead, it acts like SNES/Super Famicom hardware and then upconverts the video output to the desired resolution over HDMI. So while you have full control over resolution and upscalers, there are no emulator tricks like save states or rom patches. When you put a cartridge in the system, you play that game just as though you would on a SNES.

When you put a cartridge in the system, you play that game just as though you would on a SNES.

GAMEPLAY

SNES and Super Famicom games look and play excellent on the Super Nt. Like the original Nt, the Super Nt uses immaculate video processing to upconvert ordinarily SD or sub-SD SNES games to up to 1080p. Without an upscaler filter, that means clean lines between contrasting pixels, each displayed in bright, vivid colors. It makes older games look fantastic on a modern TV, comparable with emulation-based systems that simply render the games at higher resolutions, such as the SNES Classic.

The games play very well, too. Animation is smooth and steady, with no noticeable lag (though there might be input lag on your TV's end as high as 100ms; remember to set your TV to Game Mode if it has one). Analogue sent us an 8bitdo SN30 and Retro Receiver for use with the Super Nt, and it performed responsively even over a wireless Bluetooth connection.

I tested the Super Nt with Disney's Aladdin, Killer Instinct, and Super Mario All-Stars for the SNES, and Star Fox, Wildtrax (Stunt Race FX in North America), and Yoshi's Island for the Super Famicom. They all ran perfectly, with responsive performance and controls.

THE BEST AT WHAT IT DOES

The Analogue Super Nt is a remarkable little retro console for a very specific audience. It can play only SNES/SF games, unlike the Super Retron Trio Plus, and it doesn't have many built-in games, unlike the SNES Classic. But its build quality and graphics processing are top-notch. That's the most important aspect of the Super Nt: You can play your own classic 16-bit games on your modern TV with flawless upconversion. Its price is high even compared with other enthusiast-level retro game systems including the Japanese Retro Freak, but unlike those other systems, the Super Nt doesn't rely on emulation, which will please retro game purists. If you want the best classic gaming experience with your cartridges and don't want to touch emulators, the Analogue Super Nt is your best option, and it's our Editors' Choice.

WILL GREENWALD

DJI Mavic Pro Platinum: The Best Small Drone

PC MAGAZINE EDITORS' CHOICE

The DJI Mavic Pro Platinum is the best small drone you can buy. Its folding form factor lets you stow it easily in a camera or messenger bag, and it has a dedicated remote that's also quite compact. The drone's flight performance is top-notch, with 4K video to match, and built-in safety features including automated return-to-home and forward obstacle avoidance. It's a fantastic choice for most aerial videographers and YouTubers, and it's our Editors' Choice—although DJI has some options to cater to the higher end, including the Phantom 4 Pro and Inspire 2.

DJI Mavic Pro
Platinum
$1,099.00

DESIGN

The Mavic Pro Platinum is the second iteration of the Mavic drone. DJI didn't make any changes to the basic design aside from a lighter silver finish; you can't tell it apart from the Mavic Pro (which is a darker gray) by sight. When folded, the drone measures 3.3 by 3.3 by 7.8 inches; it weighs about 1.6 pounds. It fits into the pocket of my camera bag in which I normally stow a small telezoom lens. That's a big difference from the Phantom 4 Pro, which really requires its own backpack to transport.

A drone shot can add some serious production value to your vlog or independent film project. Having one that you can throw in a backpack, get up in the air in minutes, and fly in tight spaces—thanks to its size and forward obstacle avoidance—is a big deal. And the Mavic is just so much easier to travel with than a Phantom.

It's also easier to set up. The Mavic's propellers fold, so you don't need to remove them for storage (two sets are included). The Phantom uses fixed props that are easy to install—they click and lock rather than screw into place—but even so, they add a few minutes to the flight-prep process.

DJI Mavic Pro

Platinum

PROS Compact, folding design. Small remote control. Forward obstacle avoidance. Automated flight options. Crisp 4K video. 12MP Raw and JPG stills. Up to 28 minutes of flight per charge.

CONS Pricey. Frequent firmware updates. Requires a smartphone for full experience.

The Mavic Pro Platinum has a lighter finish than the original Mavic Pro but is otherwise physically identical.

The Pro Platinum promises two upgrades over its predecessor: Those are longer flight times and quieter operation. Both result from refinements in motor and propeller design.

In our battery tests, the drone averaged about 28 minutes of flight time on a fully charged battery. That's a little shy of DJI's 30-minute estimate but a big improvement over the 23 minutes we got, on average, with the original Mavic Pro. It's still a good idea to carry a spare battery (or two). Extra batteries are $89, and DJI sells the Mavic Pro Platinum Fly More bundle for $1,399, which adds two extra batteries (for a total of three) as well as a carrying case, an additional spare propeller pair, a car charger, and a charging hub.

Built-in safety features include automated return-to-home and forward obstacle avoidance.

When folded, the Mavic Pro fits easily into a camera bag. It's not that much bigger than a telezoom lens.

The drone gathers information data from both GPS and GLONASS satellites. It picks up the location very quickly and can hover in place thanks to the precision that satellite positioning provides. The Mavic can also fly indoors without the aid of satellites. It has downward-facing sensors that read the patterns of the ground below to keep it steady during indoor flight. You should avoid flying over mirrored surfaces and give yourself plenty of room.

The Mavic cruised along at a steady 20mph in test flights with obstacle avoidance enabled. It has a Sport mode that disables the obstacle sensors and pushes the top speed to 40mph. The Phantom 4 Pro gives you a bit more speed in the air, 31mph in its standard mode and 45mph in Sport. The extra speed can add some oomph to your aerial videos, but remember that you can always speed up video using Premiere Pro.

DJI GO APP AND REMOTE CONTROL

The Mavic Pro Platinum ships with the same compact remote control as its predecessor. The remote is about the size of a game controller when folded. It has a monochrome LCD display (which shows connection status, battery life, and the like) and two analog sticks for flight control. Buttons include Power, Return-to-Home, and Pause. Control wheels adjust camera exposure and gimbal tilt, and there's a small joypad on the face with custom functions assignable via the DJI Go 4 app. The remote also has video record and still-photo buttons.

“You can fly the Mavic without a smartphone, but then you won’t get a first-person view from the camera.”

The remote has a bottom clip that unfolds to hold a smartphone. It can easily fit a big one like the iPhone 8 Plus. A USB cable runs from the side and through the clip to connect your phone to the remote. DJI includes Lightning, micro USB, and USB-C cables, so all modern smartphones are covered. Getting the cable threaded through and locked into position can be a bit tricky, but once it's in place, you won't have to worry about it.

You can fly the Mavic without a smartphone, but you won't get a first-person view from the camera, and you won't have access to adjust a lot of its video and photo features. I recommend you use your phone with the remote; the safety benefits of seeing through the drone's camera are reason enough.

> **I used an iPhone 8 Plus in testing, but any modern Android or iOS handset will do the trick.**

You'll need a phone that can run the DJI Go 4 app. I used an iPhone 8 Plus in testing, but any modern Android or iOS handset will do the trick. Android devices need to be running version 4.4 or newer; iOS needs version 9.0 or newer.

In addition to a live feed from the Mavic's lens (at 720p quality), the app enables use of automated flight modes and lets you configure the obstacle avoidance system and set video and image capture settings. Automated flight patterns include Point of Interest, which flies around a point in a perfect circle; Waypoints, which can fly a preset pattern repeatedly; and Follow Me, which follows the position of the remote control.

You also get TapFly, which lets you fly the drone by tapping on the screen of your phone rather than using the flight sticks, and Course Lock and Home Lock, which change the way the way the drone responds to stick commands based on its orientation or position in relation to your current location.

Automated subject tracking is another option. ActiveTrack lets you draw a box around a subject. The drone will track the subject as it moves and use its obstacle avoidance system to prevent crashes.

FAA regulations require you to keep the drone in your line of sight when flying. In the event you're working with a spotter or flying in a locale with less strict rules, the Mavic is capable of going much farther. DJI rates its transmission range in terms of miles, so you won't have to worry about losing the video feed when flying. In the unlikely event that communication is disrupted, the Mavic Pro returns to its take-off point and lands itself.

There's been a lot of noise over DJI's firmware updates and No-Fly Zone enforcement since we last evaluated one of its products. Let's talk firmware first.

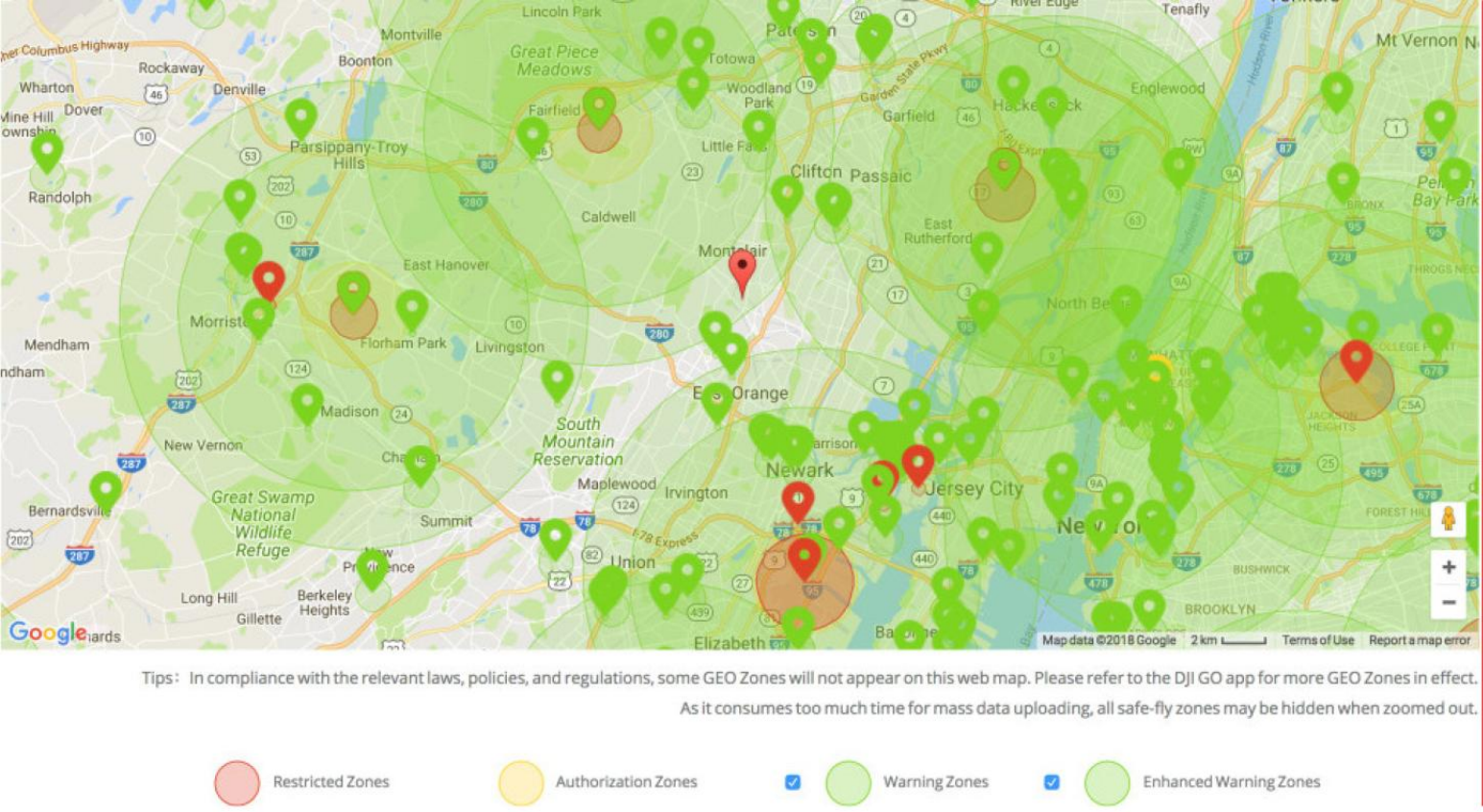
DJI pushes out firmware updates with regularity. And because you use an internet-connected phone to run the DJI Go 4 app, it knows if there's new firmware available.

Typically you can bypass the update in the field and go flying, but some past updates have prevented flight. But keeping up to date with firmware is a good thing. Bug fixes are implemented, new features are added—typical firmware stuff.

Frequent fliers can stay on top of updates, but what if you use the drone only a few times a year? You're probably going to have to update before most flights. Schedule an hour to do so the night before flights, so you can avoid getting into the field to find the Mavic Pro isn't ready to fly.

No-fly zones are another bone of contention. DJI has taken a more hands-on approach to limiting flight in order to force its customers to comply with FAA regulations. The drone won't take off in some areas at all—DJI refers to these as Restricted Zones. These include all of Washington, DC and the immediate area around major and minor airports. If you do have authorization to use the drone in these normally verboten airspaces, you'll need to contact DJI via email to arrange a flight.

Then there are Authorization Zones. You can unlock these via the app, assuming that you have verified your DJI account. Some of these change based on events—I'm seeing one in Manhattan for VIP Movement at press time—but others are static. DJI gives a model aircraft flying club as an example of a typical Authorization Zone; these are often situated near small airfields.



This is the DJI Fly Safe Geo Zone Map. The company implements zones that prohibit flight near airports, power plants, prisons, and so on, and temporarily creates zones around major stadium events, forest fires, and other emergency situations.

Finally there are Enhanced Warning Zones, which you can unlock without a verified account, and Warning Zones, which blanket the United States but don't prevent you from taking off. The DJI Go app warned me that there are unpaved airstrips near my parents' rural Pennsylvania farm, my preferred testing area for first flights, which is news to me.

DJI has an interactive map that breaks down all of these areas. It's worth a look before you buy the Mavic Pro Platinum. You don't want to jump into drone ownership only to find that your home area is riddled with flight restrictions.

Preventing drone owners from flying where they shouldn't is a divisive issue. Those who fall on the more libertarian side of things philosophically will see it as an overstepping of government bounds. DJI is a private entity, but the flight restrictions are based on data from the FAA.

The other side of the argument is that the app can keep you from getting into some serious trouble. Ignorance is not a defense if you're caught flying in an area where you shouldn't be, whether over a wildfire or a military base. An aerial video or photo is not worth jail time.

VIDEO AND IMAGE QUALITY

The imaging capabilities of the Mavic Pro Platinum haven't been upgraded. It uses the same nose-mounted camera, stabilized using a 3-axis gimbal. It covers a field of view about the same as a 25mm lens on a full-frame camera—a wide angle, but not an ultra-wide one—and can record 60Mbps 4K video as well as JPG and Raw (DNG) still images.

Video quality is excellent, with crisp details and a number of looks, including a flat color profile, available. The gimbal does a fine job keeping footage smooth and steady. Image quality is on par with a point-and-shoot camera (the image sensor is a 12MP 1/2.3-inch CMOS design).

It's very good, and quite printable, in bright light. If you're concerned about shooting at a high ISO, the 1-inch sensor used by the Phantom 4 Pro and Advanced will do a better job, and give you more resolution at 20MP.

In addition to shooting in landscape orientation, the Mavic Pro Platinum can rotate its lens and shoot in portrait mode. This is more useful for stills than for video. It's not a feature I used that often—I tend to prefer wide landscape shots in the wider landscape orientation, and when shooting straight down, it's not required. But it's nice to have.

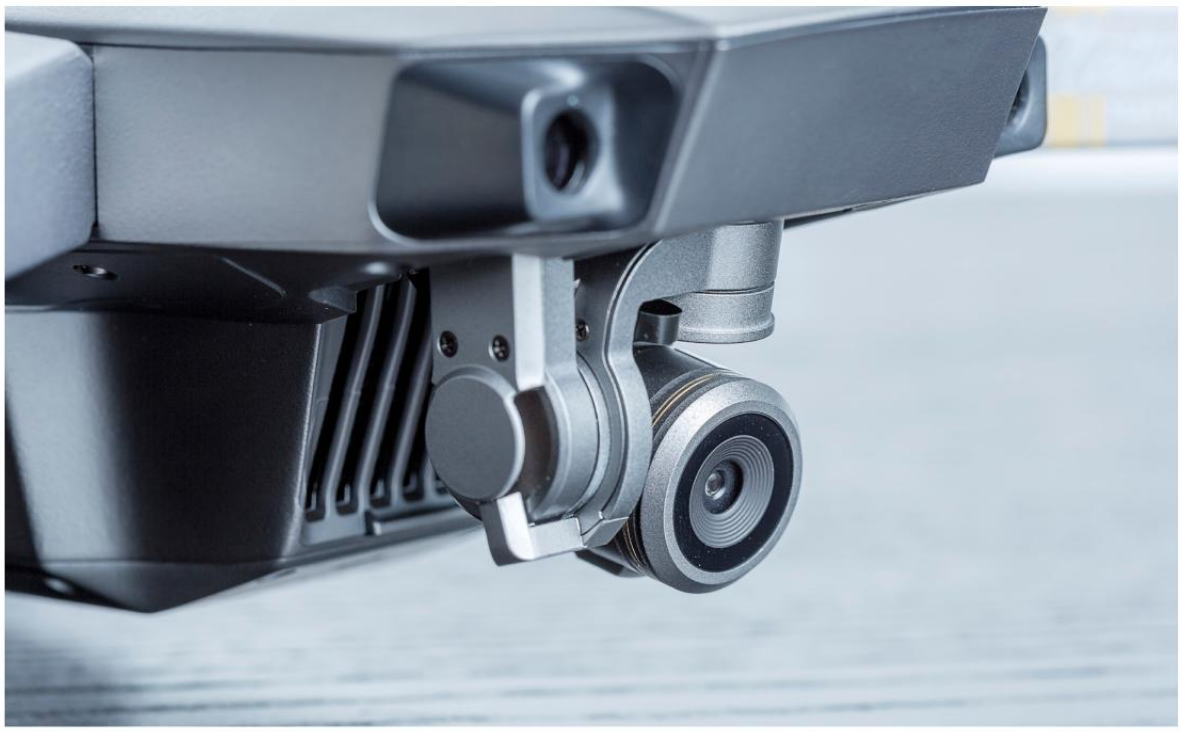
Video quality is excellent, with crisp details and a number of looks, including a flat color profile, available.

Video options include UHD 4K at 24 or 30fps, DCI (the wider cinema 4K format) at 24fps, 1080p at standard frame rates up to 60fps and at 96fps for slow-motion playback, and 720p at up to 180fps.

The Mavic camera supports focus adjustments, which isn't the case with every drone camera—many are fixed focus, so you never have to worry about setting a focus point. If your footage isn't looking clear, tap on a distant subject on the screen to reacquire focus.

CONCLUSIONS

The DJI Mavic Pro Platinum is the best small drone on the market. Its folding design makes it a go-anywhere option that's easily stowed into a gear bag. It's a bit quieter and flies longer than the original Mavic Pro, but it also costs more. Don't rule out the first version, especially if you're on a budget and don't mind a slightly shorter flight time.



> **If you're after a compact quadcopter for vlogging, video, and photography, the Mavic Pro Platinum is what you want.**

Video and image quality are solid, as good as other DJI models with similar image sensor designs—this includes the Phantom 3 line and the first version of the Phantom 4. If you need something beyond that, the Phantom 4 Pro and Advanced models offer a 1-inch image sensor camera like you find in high-end compact cameras, and you can configure the pro-grade Inspire 2 with an SLR-sized APS-C camera, the Zenmuse X7.

If you're after a compact quadcopter for vlogging, video production, and photography, the Mavic Pro Platinum is what you want—but it's expensive. DJI does sell another small model, the Spark, which is now available for less than its $500 MSRP. The Spark is OK for casual use, but its flight time is very short, and video is just 1080p. It packs a lot of tech into a small frame, but it's more of a toy than a real creative tool. So while the Mavic Pro Platinum is pricey, it's the best of the bunch and our Editors' Choice.

JIM FISHER

Panasonic Lumix DMC-FZ80: A Ton of Zoom at a Great Price

We liked the Panasonic Lumix DC-FZ70 thanks to its long zoom lens, low cost, and strong image quality. But it had some serious shortcomings in the bells-and-whistles department. The DC-FZ80 keeps the same lens and ticks up the price, but for the extra money, you get Wi-Fi, a better EVF, a touch LCD, and 4K video capture. It's a better overall camera, though not quite our favorite bridge superzoom. The Canon PowerShot SX60 HS is still our Editors' Choice, but the Panasonic is a good—and cheaper—alternative.

Panasonic Lumix
DMC-FZ80
$399.99
●●●●○

DESIGN

The FZ80 is a typical bridge point-and-shoot. It marries a small (1/2.3-inch) image sensor to a big zoom lens, putting the two together in a body that's about the size of a small SLR. Putting that glass in front of a sensor type developed for pocket-friendly cameras allows for an incredible zoom range, much more than you'd get from any SLR lens, in a package that measures 3.7 by 5.1 by 4.7 inches (HWD) and weighs about 1.4 pounds.

The fixed lens covers scenes from an ultra-wide (20mm full-frame equivalent) perspective when zoomed all the way out. It extends to a beyond-extreme telephoto (1,200mm) at its maximum extension. This gives the lens an advantage in telephoto reach over pocket cameras—models such as the Sony HX90V reach about 720mm—and also covers a wider angle. The FZ80's 20mm lens is significantly wider than the more typical 24mm at which most compact cameras start.

Physical controls are supplemented by the Panasonic Q.Menu. Every camera maker has its own take on this interface, which shows translucent shooting controls over the live view frame, so you can make adjustments to settings without losing sight of what your lens is seeing. The FZ80's menu is customizable and can be navigated using rear control buttons or via touch.

Panasonic Lumix
DMC-FZ80

PROS Huge 60x zoom range. Fast autofocus. 10fps Raw capture. 30fps 4K Photo capture. Touch LCD. Sharp EVF. Wi-Fi.

CONS No EVF eye sensor. Fixed rear LCD. Limited Raw buffer. Omits 24fps video capture. Telephoto video shows wobble effect.

The Lumix DC-FZ80's lens extends significantly to net 1,200mm reach.

The rear LCD is a fixed panel, unlike the more useful vari-angle display offered by the Canon SX60 HS or Panasonic's own premium FZ1000. It is quite sharp, however, at 1,040k dots packed into a 3-inch frame. And it is sensitive to touch, so you can tap to set a focus point or navigate menus as you would with a smartphone.

The camera also has an eye-level electronic viewfinder (EVF), something you really need with such a long zoom lens. Even with in-camera stabilization, it's easier to get a sharp zoomed shot with the camera raised to your eye than it is holding it at arm's length. It has no eye sensor, so you use a button to switch between the EVF and LCD.

The rear LCD is sensitive to touch, so you can tap to set a focus point or navigate menus as you would with a smartphone.

CONNECTIVITY

The FZ80 has Wi-Fi for image transfer and remote control. It works with the Panasonic Image App, a free download for Android and iOS that lets you copy photos from the camera to your phone for editing and sharing, and it also offers full manual control and a live feed so you can use your phone as a remote control.

The 3-inch LCD is sensitive to touch, but it doesn't tilt.

On the body are micro HDMI and micro USB ports, the latter used for in-camera charging. The camera is rated to nab about 330 shots using the rear LCD or 240 shots using the EVF, both solid marks for a bridge model. The ability to add juice via a USB power bank is certainly a benefit for travelers; if you're the type of photographer to carry a spare battery, it's wise to invest in an external charger as well, so you can charge one in the camera and one out of the camera concurrently.

PERFORMANCE AND IMAGING

The FZ80 takes a little time to turn on, focus, and fire—about 1.8 seconds—because its lens has to move in position to grab an image. But once it's ready to go, it's quite speedy. The autofocus system locks on in about 0.05-second at both the wide and telephoto end in bright light. In dim conditions, it takes about 0.9-second to focus and fire at the wide end and tends to hunt when acquiring focus at 1,200mm. A bridge camera isn't the the best choice for shooting in low light unless you opt for a model with a larger 1-inch sensor and shorter zoom lens, such as the Panasonic FZ1000 or Sony RX10.

Burst shooting is available at about 10fps at full 18MP resolution in Raw or JPG format. You can snap 13 Raw+JPG, 15 Raw, or 52 JPG shots at a time, with about 15 seconds required to clear the buffer after a Raw burst and about 8 seconds to do the same for JPGs. The camera supports Panasonic's 4K Photo mode as well, which can shoot 8MP JPGs at 30fps with your choice of fixed focus through the burst or Panasonic's Post Focus mode, which changes the active autofocus point between each shot.

Tracking focus is available when you're shooting full-resolution files. Setting the camera to AF-C will cause it to acquire focus for each shot in a burst, but it does slow the capture rate down. You're limited to shooting at 5.4fps when tracking moving subjects. It works well, though, delivering solid results in our lab tests and in the field, where we used the FZ80's long lens to snap shots of bald eagles in flight.

I used Imatest to check the sharpness of the FZ80's lens. At its widest angle and aperture, 3.6mm f/2.8, it matches the field of view of a 20mm lens on a full-frame camera. It scored 2,078 lines per picture height on a center-weighted sharpness test, better than the 1,800 lines we want to see out of a camera of this type with an 18MP image sensor.

The camera's top plate houses a hot shoe, so you can connect an external flash . Right in front of it is a pop-up flash.

At the 140mm equivalent position, the maximum aperture is f/5.3. Image quality remains solid at 1,811 lines. Zooming farther, to the 235mm equivalent focal length, cuts the maximum aperture to f/5.5, but resolution remains strong at 2,007 lines. Testing beyond that is impractical in our lab—there's simply not enough room to back up from the test chart and keep it in frame.

I shot numerous images at full zoom in the field. The lens certainly loses some sharpness at its maximum extension. If you're hoping to make big prints of a handheld shot of the moon, you'll be disappointed. But the results are very Instagrammable.

Imatest also checks photos for noise. Noise can detract from detail and add a grainy quality at higher ISO settings. When shooting JPGs, the FZ80 keeps noise under 1.5 percent through ISO 1600, so you shouldn't have trouble capturing low-noise images in sunlight, even when keeping the shutter speed short to freeze motion.

Although the camera controls noise through ISO 1600, that doesn't mean image quality is perfect through that setting. In reality you can shoot through ISO 400 without any noticeable drop in quality. There's some mild smudging of fine detail at ISO 800, which is more prevalent at ISO 1600. Results at ISO 3200 and 6400 are noticeably blurred.

Those who are really serious about images can set the FZ80 to capture photos in Raw format. Raw images require post-processing before sharing, but they hold up better than JPGs at higher ISO settings. You see a lot of grain at ISO 1600 when shooting in Raw, but detail holds up well. But you don't want to push too far beyond that—grain starts to overwhelm the image at ISO 3200, and at ISO 6400 it's even more distracting.

The FZ80 shoots video at 4K resolution at a fixed 30fps frame rate and 100Mbps compression rate. You can also shoot at 1080p at 60fps (28Mbps) or 30fps (20Mbps), and at 720p at 30fps (10Mbps), all in MP4 format. It also supports AVCHD compression but only at 1080p quality. The camera has no 24fps option, a downer for those who prefer video with a cinematic look.

At wide angles, video looks quite good, with crisp detail and strong colors. But the limitations of optical stabilization for handheld video show when zoomed in. Handheld footage at extreme zoom levels, beyond 500mm, show significant wobble. You'll want to use a tripod to steady the camera when recording at extreme focal lengths.

You'll want to use a tripod to steady the camera when recording video at extreme focal lengths.

CONCLUSIONS

The Panasonic Lumix DC-FZ80 delivers an incredible amount of zoom coverage for not a lot of money. It uses the same lens as its predecessor but improves on fit and finish, with a better, touch-enabled rear LCD; a sharper EVF; Wi-Fi; and 4K video, all missing on the bargain-oriented FZ70. The FZ80 costs about $100 more, but at $400, it still falls well into the range of affordability, especially given how far a reach the lens delivers. You can spend a bit more on our Editors' Choice, the Canon PowerShot SX60 HS, which has a similar zoom range and adds a vari-angle LCD. If you're able to spend even more for a superzoom model, consider one with a 1-inch sensor, such as the Panasonic FZ1000 or any member of the Sony RX10 series.

JIM FISHER

Canon Pixma TS8120 Wireless Inkjet All-in-One

Canon Pixma TS8120 Wireless All-in-One

$179.99

●●●●○

One rung down in Canon's lineup from the Pixma TS9120 Wireless All-in-One Inkjet Printer—our Editors' Choice consumer photocentric all-in-one printer—stands the Canon Pixma TS8120 Wireless Inkjet All-in-One, and it stands tall. It has all its prizewinning sibling's printing chops, thanks to its six ink tanks, and prints excellent text and very good graphics. The TS9120 is more versatile, thanks to its inclusion of Ethernet connectivity, and retains its Editors' Choice, but if you can make do with USB and Wi-Fi, you can save a little money with the TS8120 and get an excellent household printer.

BUILT FOR THE HOME

A three-function all-in-one printer, the TS8120 is able to print, scan, and copy but not fax. It has a handsome (if basic) design and comes in a choice of three colors: white, red, or black. The printer measures a compact 5.5 by 14.7 by 12.8 inches (HWD), and weighs 14.4 pounds. The front panel, which can be tilted upward for easy access, includes a 4.3-inch color touch LCD, a little smaller than the 5-inch display on the Canon TS9120. To the left of the output tray is a slot for memory cards in the SD family.

Paper capacity is 200 sheets, between a 100-sheet main tray and a 100-sheet rear feeder (which can also fit up to 20 sheets of letter-size photo paper. The TS8120 also includes a tray for direct printing onto optical discs. It has an auto-duplexer for two-sided printing. On top is a letter-sized flatbed scanner, which lacks an ADF.

Canon Pixma TS8120 Wireless
All-in-One

PROS Excellent text quality. Very good photo and graphics capabilities. Compact and lightweight. SD card slot. Appealing design.

CONS Lacks automatic document feeder (ADF). No Ethernet connectivity. No fax capability.

MOBILE PRINTING FEATURES

The TS8120 can connect directly to a computer via USB or to a network via Wi-Fi, and it supports printing from or scanning to a mobile device from the Canon Print app. It also supports Pixma Cloud Link, which enables you to access your files directly from a variety of photo-sharing, social networking, and storage sites. Unlike the Canon Pixma TS9120, it lacks Ethernet connectivity. I tested it over a USB connection with drivers installed on a PC running Windows 10 Professional.

SOLID SPEED

Printing speed is fine for a home inkjet all-in-one. In printing the text-only (Word) portion of our business applications suite, it averaged 13.1 pages per minute (ppm), and 4.7ppm in printing our full business suite, which includes PDF, PowerPoint, and Excel files in addition to the aforementioned Word document.

These scores effectively match those of the Canon TS9120, which we timed at 13.2 and 4.7ppm on the Word document and full suite. The Canon Pixma TS8020 was a bit slower in printing out both our Word document (11.4ppm), and the entire suite (4.4ppm). In printing photos, we clocked the TS8120 at 38 seconds per print, a little off from the TS9120's 32-second clip but still a very respectable speed.

> **A three-function all-in-one printer, the Canon Pixma TS8120 is able to print, scan, and copy but not fax.**

DAZZLING OUTPUT

The six ink tanks that the TS8120 uses include both dye- and pigment-based black inks (which helped it excel in both photo and text printing) in addition to the usual cyan, magenta, and yellow, plus photo blue. The TS8120's overall output quality, based on our testing, is well above par for an inkjet, with excellent text and very good photos and graphics. Text quality is among the best I have seen for an inkjet and better than many lasers, and should be good enough for any business use, even ones requiring small fonts.

In printing the graphics part of our suite, colors were generally well saturated. The TS8120 did well with thin colored lines and in differentiating between similar tones. Some backgrounds showed a faint trace of banding (a regular pattern of striations), but it's inconspicuous enough that only the pickiest recipients of your printouts would likely notice. We noted some dithering in the form of graininess in some illustrations, but it was relatively mild.

The wireless printer has a handsome (if basic) design and comes in a choice of three colors: white, red, or black. It measures a compact 5.5 by 14.7 by 12.8 inches (HWD), and weighs 14.4 pounds.

Our test photo prints were of the high quality we've also seen with the Canon TS9120 and TS8020. Colors were vibrant, and there was good retention of detail in both bright and dark areas. The only issue worth noting was a slight tint on a monochrome print.

A SUPERB HOME ALL-IN-ONE

The only thing standing between the Canon Pixma TS8120 Wireless All-in-One Inkjet Printer and an Editors' Choice is the fact that our current top pick—the Canon Pixma TS9120—adds Ethernet connectivity and a slightly larger display for just $20 more. That said, with improvements in Wi-Fi technology, Ethernet is not as important as it was a few years ago, and many thin-and-light laptops have done away with Ethernet ports.

If you don't need Ethernet, there's no reason to pay for it, and you can get a terrific home all-in-one printer with great output quality across the board at a reasonable price in the TS8120. Keep in mind that the TS8120 is a home printer, and in addition to Ethernet eschews some primarily office-centric features such as fax, an automatic document feeder, and a port for a USB thumb drive, all of which you'll find on the Brother MFC-J985DW, our Editors' Choice inkjet all-in-one for home or home office.

TONY HOFFMAN

HP EliteOne 1000 All-in-One Lets You Upgrade Components

PC MAGAZINE EDITORS' CHOICE

Although the HP EliteOne 1000's gorgeous 27-inch 4K display and thin bezels are visually impressive, they aren't necessarily unique. But this business-oriented machine does have one killer feature that is rare among all-in-ones: easy upgradeability. In fact, it's so easy to access the components in the EliteOne 1000—and even to remove the display—that both IT departments and consumers might consider buying it instead of a traditional desktop. It also happens to include many of the internal components of the same-price Apple iMac 21.5-inch, which makes it an excellent value and our new Editors' Choice for midrange AIOs.

HP EliteOne 1000
All-in-One

Starts at $1,279.00;
$1,519.00 as tested

●●●●○

ALL ABOUT THAT BASE

Instead of housing the Intel Core i5 processor, 256GB M.2 SSD, and 8GB of RAM inside the display enclosure, HP has placed these and the rest of the components into the EliteOne 1000's base. That's the secret to the computer's easy upgradability, but it also means the base is much bigger than the ones on the iMac or the Dell Optiplex 7450 All-in-One. It's wedge-shaped, sloping from back to front, and it measures 1.5 by 15.7 by 7.5 inches (HWD). Along the front of the base are a physical power button and a few virtual buttons designed to work with Skype for Business (for example, ending a call and muting the microphone) as well as a virtual slider to control the system volume. All of the buttons are LED-backlit.

Above the button row is a massive speaker grille that runs the entire width of the base, complete with a Bang & Olufsen logo. Unfortunately, the size of the speaker grille and its branding are a bit misleading, since all you get are two small stereo speakers occupying the left and right corners of the base. They're fine for videoconferencing, but they don't deliver robust bass, certainly nowhere near as astonishing as the output from the 10-speaker setup on the much more expensive Dell Precision 5720. Still, the size and placement of the speakers make sense when you consider that in return for so-so audio quality, you get a gorgeously thin display enclosure.

HP EliteOne 1000
All-in-One

PROS Beautiful 27-inch 4K display. Dual webcams slide behind display when not in use. Fans are whisper-quiet. Easily upgradable. Relatively inexpensive.

CONS Uncomfortable mouse and keyboard. Anemic stereo speakers.

Not only does the display look sleek, but it also measures just 14.4 by 32.1 by 2.9 inches, which is very petite for a 27-inch screen. That's thanks to narrow bezels and a unique webcam module that pops up from behind the screen and then retracts again when not in use. There are actually two 2MP webcams on this module, one forward-facing and one rear-facing, which could come in handy if you plan to use the EliteOne 1000 at, say, a conference registration table to take ID photos of attendees. The HD video the cams offer is perfectly adequate for videoconferencing, although it's not quite as sharp as the 1080p HD webcam on the Apple iMac Pro.

The screen is a WLED panel with a matte finish to guard against reflections, and it's very bright.

The screen is a WLED panel with a matte finish to guard against reflections, and it's very bright. It's so luminous, in fact, that I set its brightness level to 40 percent even while I was testing it in the harsh fluorescent light of PC Labs (you can't adjust brightness using Windows; all the screen adjustments are accomplished using four dedicated physical buttons on the bottom edge of the display and an OSD interface). The display also has in-plane switching (IPS) technology to prevent the colors from washing out as you move your head.

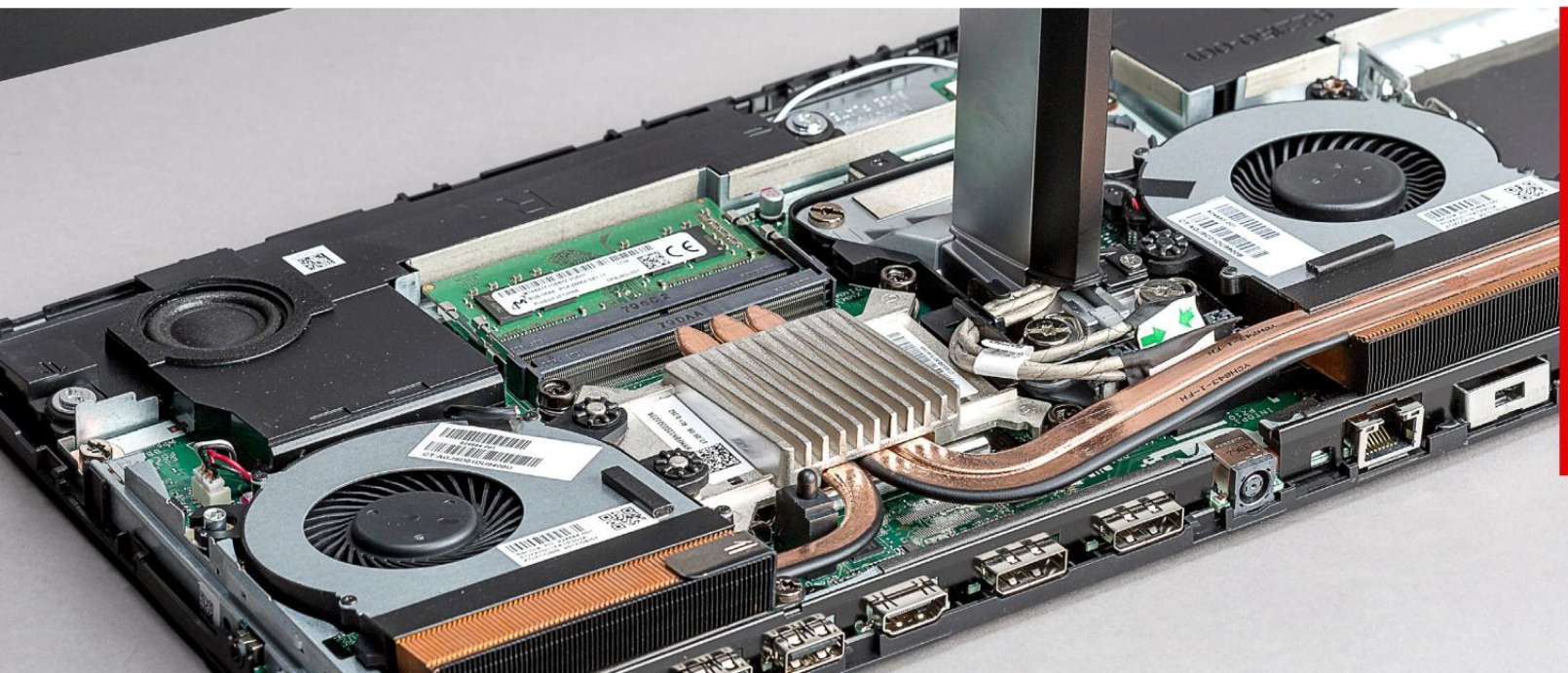
I was initially worried that the integrated Intel HD Graphics 630 in the EliteOne 1000 would be too anemic to power such a large 4K screen. Indeed, most other midrange all-in-ones include a discrete GPU, such as the iMac's AMD Radeon Pro 560. I was proved wrong over several days of testing, however. As long as you stick to basic productivity apps, web browsing, and videoconferencing, you'll have a very smooth and enjoyable 4K experience.

When you add everything up, the entire system (base and screen) measures 18 by 24.2 by 7.5 inches and weighs 22.8 pounds. That's slightly slimmer but a bit heavier than the 27-inch iMac, which is 20.3 by 25.6 by 8 inches and 20.8 pounds. It's much lighter than the 37-pound Precision 5720, which is laden down by its array of speakers and articulating stand. HP also offers a 23.8-inch version of the EliteOne 1000 with the same configuration but without a 4K display, for $1,279.

MAJORLY UPGRADEABLE

Like the speakers, the EliteOne 1000's relatively inflexible stand (it can tilt the display only a few degrees) is another limitation of the upgradable design. But for many, that upgradeability factor is this all-in-one's best feature. Here's why.

The most iconic all-in-one, the iMac, is designed to be impossible to upgrade yourself, save for simple memory swaps. The iMac Pro eliminates access to even the memory modules, and though the OptiPlex 7450 and Precision 5720 both have user-accessible components, they're not exactly easy to access. Enter the EliteOne 1000, which has a cover that comes apart with no tools required. Just press the two release buttons on the rear of the base unit to lift away the rear portion of the cover, and then press the release buttons on the front cover and lift it straight up to remove it. Voila: You can now see and access virtually any system component.



Some of this all-in-one's components are hidden beneath the cooling system and will require tools to access.

Memory can be added with no further tools required, and so can a 2.5-inch hard drive or SSD. Our review unit has the 2.5-inch bay at the left of the PC vacant, relying exclusively on an M.2 SSD located on the motherboard.

Once you're ready to retire the EliteOne 1000, you can even remove the display and just dispose of the base. It takes roughly eight steps and no tools to do so. Some upgrades will need tools, of course, and some may necessitate removing one or both of the cooling fans to access the components beneath them. But on the whole, this is a very well-thought-out and accessible case, rivaling many traditional small-form-factor business desktops.

HP, of course, hopes that the EliteOne 1000's easy upgradability will drive more sales from IT departments who have previously been wary of all-in-ones. It's a marketing tactic, to be sure, but a useful one. Add in the system's eye-catching design and 4K screen, and the machine will be a pleasure to use as well, whether it's in a cubicle or on your kitchen counter at home.

I do have a few minor design quibbles. The wireless keyboard and mouse HP includes with the system are ho-hum. Their plasticky feel and uninspired design make the peripherals look downright ugly compared with the rest of the system. The peripherals that Dell and Apple include with their all-in-ones are of higher quality, and they match the design of the systems they're paired with better. You can, of course, buy a better keyboard and mouse on your own.

Most of the ports are at the rear of the base, making them a bit farther away and harder to access than the ports of the iMac, which are located on the lower left edge of the display. Fortunately, HP has added a few of the most-used ports in a more easily accessible location at the base's right edge. These include a USB 3.1 port, a USB-C port, and a headphone jack. Around back are four more USB 3.1 ports, HDMI and DisplayPort outputs, a DisplayPort input, a gigabit Ethernet port, and the power connector. Wireless connectivity includes 802.11ac Wi-Fi and Bluetooth 4.1.

The EliteOne 1000 has a generous warranty that offers three years of coverage for parts and labor as well as on-site repairs.

SOLID PROCESSING POWER

To add a top-notch Ryzen 7 or Core i7 processor and a discrete GPU to the already excellent and reasonably priced EliteOne 1000 would be a tall order, and it's no surprise that HP doesn't do this. If the company had tried, it probably would have had to sacrifice on design and ended up with something like the Acer Aspire Z3, which has more powerful components but looks tired and feels cheap.

Still, the Intel Core i5-7500 running at 3.4GHz is no slouch. It's the same CPU inside the 21.5-inch iMac, which costs almost exactly the same. The processor is a bit slower in the HP than it is in the Apple on our Handbrake video-encoding test (a minute and four seconds vs. 1:14) and our collection of Photoshop image-editing tasks (3:08 vs. 3:19). But you shouldn't buy this computer for heavy image or photo editing; leave that to the much more expensive iMac Pro or Dell Precision 5720. The EliteOne 1000's score of 2,937 on the all-encompassing PCMark 8 benchmark indicates that it's a solid performer for the more basic tasks that its users are likely to perform every day, like word processing, Skype sessions, web browsing, and the like. It's worth noting, too, that even when performing more intense tasks, there was little to no fan noise.

> **I do have a few minor design quibbles. The wireless keyboard and mouse HP includes with the system are ho-hum.**

Perhaps the biggest area in which HP skimps in order to be able to sell this PC for less than $1,500 is graphics horsepower. It's the only system among the peers we tested to include an integrated GPU, which shares resources with the main processor. The result is a machine that can't reliably be used for gaming, even at medium quality settings and lower screen resolutions. We look for frame rates of above 30fps (frames per second) on the Heaven and Valley benchmarks, and the only comparable systems to post these numbers were the iMac and the Optiplex 7450, thanks to their AMD Radeon GPUs. To compound the problem, an off-the-shelf GPU is perhaps the most important component that you can't add to the EliteOne 1000, since it has no PCI slots.

I saw no lag while resizing app windows, one of the most difficult tasks for an integrated GPU to perform at 4K resolution.

Still, the Intel HD Graphics 630 chip is fine for everyday tasks. In testing, I experienced no lag while resizing app windows, one of the most difficult tasks for an integrated GPU to perform at 4K resolution.

MORE VALUE FOR THE MONEY

The iMac is a beautiful feat of engineering, and it's the yardstick by which all other premium all-in-one PCs are typically measured. But the venerable Apple design hasn't changed much for more than five years, and I'd argue that the thin-bezel revolution, of which the HP EliteOne 1000 is a part, looks as good or better as any all-in-one to be dreamt up in the hallowed halls of Cupertino. If you or your business can do without a discrete GPU, the HP is the clear winner. If not, take a closer look at the iMac or competing Dell AIOs like the Precision 5720 and Optiplex 7450.

TOM BRANT

How Online Personal Tax Prep Services Stack Up

The Tax Cuts and Jobs Act, passed by Congress and signed by President Trump last December, is expected to simplify and reduce the income taxes paid by US citizens next year. While no one yet knows what the 2018 tax forms and schedules will look like, the IRS has finalized the 2017 tax year forms and schedules, and the doors are open for filing. You can still pick up paper copies at your local public library, but there's no need for that anymore. Several sites and apps make short work of simple returns for free; you can prepare and file yours in minutes—even on your smartphone.

If your financial situation involves more than, say, a W-2 and some interest income or student loan interest, you can sign up for one of the many sites that support the preparation and filing of all major IRS forms and schedules.

These online personal tax applications aren't putting all the tax-preparation professionals out of work. Though the best tax sites are capable of producing very complex returns, some individuals will still want professional guidance to ensure accuracy and avoid IRS corrections and audits.

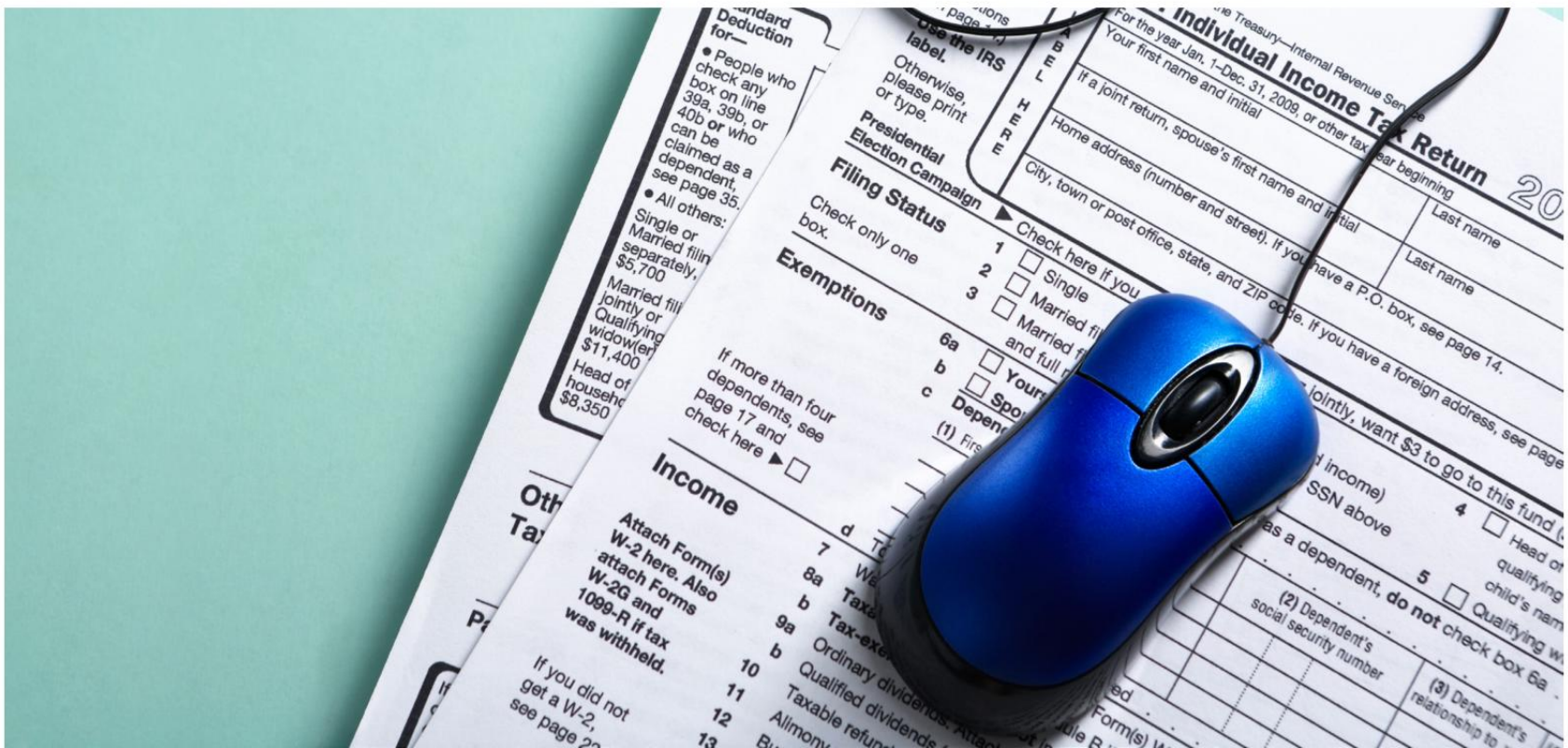
THIS YEAR'S FIELD

We tested the midrange versions of eight tax-preparation websites, the most popular options among the largest group of US taxpayers. Most of them don't tackle particularly thorny topics, such as self-employment, capital gains and losses, and rental income, but they can handle W-2s, miscellaneous income, interest income, ordinary dividends, and itemized deductions.

Every tax software company offers versions that can take on more complex incomes, deductions, and credits—in fact, more than one has introduced a new version this year designed for self-employment and the gig economy—but you pay more for this advanced coverage. Prices for the editions we reviewed range from totally free for both federal and state returns (Credit Karma Tax) to $69.95 for federal and $36.95 for state (Jackson Hewitt Deluxe).

WHAT TAX SITES DO

Personal tax preparation websites work similarly, though there are some major differences between their user experiences, the tax topics they cover, and the quantity, quality, and accessibility of the guidance they offer.



All of them act as virtual tax preparers. Instead of forcing you to see the actual IRS forms and schedules, they ask you a lengthy series of (usually) simple questions about your tax-related income and expenses. They start with your contact details and questions about your filing status and dependents. Then they launch into your W-2 and other income and proceed through any other issues that apply to you.

Tax sites follow the path of the Form 1040 (or 1040EZ) and its related forms and schedules (1099, Schedule A, Schedule B, and so on), posing relevant queries along the way. They take your responses, do all necessary calculations, and deposit your numbers and other data onto the correct, official IRS documents—all in the background, out of sight.

Once you've provided all the tax data that applies to you, these applications do three things: They check your return for potential mistakes, warning you about any errors or omissions they've found and giving you the opportunity to fix them. They transfer needed data over to any state returns you must file and help you answer any state-specific questions. Finally, they help you file your return electronically or print it out and collect any fees due.

HOW TO USE TAX SOFTWARE

These services offer two ways to move through their virtual interviews. During the early stages, after you've created a username and password and complied with any security requirements, they work like any other wizard. For some steps, they solicit personal information by providing blank fields for you to fill in. Other times, you'll select options from drop-down lists or click buttons to indicate a yes-or-no response.

When you've completed all the required information on a screen, you advance to the next, though you can back up to the previous screen when you need to. Most sites don't let you proceed until you've answered all the questions on a page; they stop you and highlight the problem. If you're not sure about a particular detail, such as an amount or the necessity of a middle initial, some sites let you bookmark or flag the page so you can move on; they then remind you to go back before you finish your return.

This navigation pattern—clicking to move forward or retreat—continues throughout each website. Once you've started entering data, other navigation options appear—toolbars that divide the site into sections, outlines of the site's tax items, lists of forms, and topics.

PROVIDING THE NUMBERS

Once you complete the personal information section, you move on and start to answer questions about your income and expenses. On some screens, you'll be responding to a basic question that doesn't require numerical data, and on others, you'll need to refer to your W-2, 1099s, and so on. You may also have to consult records you've kept throughout the year on charitable contributions and medical expenses.

Instead of forcing you to see the actual IRS forms and schedules, they ask you a series of (usually) simple questions.

Each site divides its tax content into (roughly) the logical groupings originated by the IRS: income, deductions, credits, health insurance, taxes paid, and miscellaneous issues. They all have a kind of home page for each section that displays a list of the topics covered. You click a button to start every section that applies to you, answer the questions in the miniwizard that appears, and then return to the list. The topic you just visited now has a button that reads Edit or Revisit, so you can go back and check your work and make any necessary changes.

When you finish the income section, you see a summary of what you entered there. If you're satisfied, you can move on to the deduction home page, and repeat the process until you're finished.

Some sites offer an alternative. Instead of moving back and forth to the section home pages, you can ask to visit just about every topic in one long, continuous wizard. Of course, you can click through anything that doesn't apply, but at least this shows you all the possibilities.

HELP AT HAND

Even when a query in these site's onscreen interviews is clearly worded, you might still not be sure whether you're supposed to supply information and what that information might be. Tax websites help you understand those confusing elements in a variety of ways. They might turn a word or phrase into a hyperlink that opens a small window containing a more detailed explanation. Or they might anticipate your questions and post links to related Q&As right on the pages that would spur you to ask questions.

This kind of context-sensitive help is extremely important. If you need to consult any other methods of help, it means that the service has failed to anticipate your needs, your time has been wasted, and your blood pressure has probably gone up. Sites that lack good context-sensitive help are heavily penalized in our reviews

Still, no service can anticipate every contingency or question. Most tax preparation applications offer a second tier of giant help databases of tax information that you can search if you're really stuck. Some offer glossaries, too. You may be directed occasionally to read IRS instructions or peruse an IRS publication, but that should be vanishingly rare in a good service. After all, IRS documents are free, and unless you're using Credit Karma Tax, you're largely paying for the convenience of not reading IRS documents. The IRS is, of course, the last word on taxes, but creating lucid, reassuring guides is not one of its notable strengths.

HUMAN GUIDES

If all that isn't enough, you might want to interact with a real human being. These sites offer connections to tax professionals via chat, email, or phone. If you think you're likely to need to rely on this kind of direct contact with your tax service, you're much better off doing your taxes early. Otherwise they might be overwhelmed by last-minute e-filers.

When you're using H&R Block, Jackson Hewitt, or Liberty Tax, and you're just not confident enough about some of your tax issues, you can always hand over your return to someone in one of their offices and let them take it from there (for additional fees, of course).

TurboTax provides the most innovative way to get human help. Its SmartLook feature creates a connection between you and a tax expert. You see them talking to you live on your screen. At the same time, they can see where you're having trouble by viewing your screen and troubleshooting your problem. These individuals can help you put the right information in the right place on the TurboTax site and provide some additional basic guidance, but they can't serve as tax advisors, like CPAs or EAs (Enrolled Agents) could.

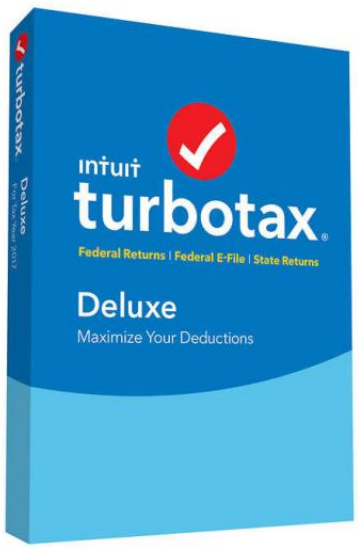
Those who anticipate needing that kind of personal service can explore the new TurboTax Live ($179.99 for federal e-filing and $39.99 per state). You'll be able to ask questions of a CPA or EA employed by Intuit as often as you need to during the preparation process. This version uses a split screen when you're getting help, so your taxes will be on one side of the screen and the friendly face of your financial professional on the other. The two of you will review your final return together before filing, and Intuit's 100% Accuracy Guarantee applies.

“The IRS is, of course, the last word on taxes, but creating lucid, reassuring guides is not one of its notable strengths.”

TAXES ON THE RUN

Probably the easiest way to prepare your taxes using one of these solutions is to plop down in front of your desktop or laptop and use their browser-based versions. But if you want to take care of this annual task while you're away from your PC, any of them can accommodate you. H&R Block, TaxSlayer, and TurboTax have mobile apps that support all major IRS forms and schedules. The other five use responsive web design, so you can view and use their sites just fine on your mobile browser.

It will be months before we see what the tax-year 2018 IRS forms and schedules look like with the new tax cuts implemented. It's taking even the professionals some time to unpack and analyze everything that's in the massive new law, but you probably have an idea already about how you might be affected, so we'd recommend you start planning before the new crop of personal tax preparation websites appears next fall.



Intuit TurboTax Deluxe 2018 (Tax Year 2017)

$59.99

EDITORS' CHOICE

●●●●◐

PROS: Exceptional user experience. Thorough interview and final review. Excellent help tools. SmartLook provides live video help from experts.

CONS: Some answers in help database supplied by non-expert users. No comprehensive navigation outline.

BOTTOM LINE: Plain-language help resources, thorough exploration of tax forms and schedules, and an unparalleled user experience make TurboTax Deluxe our top pick for tax-prep software.

TaxAct Online Plus 2018 (Tax Year 2017)

$29.95

●●●●○

TaxAct®

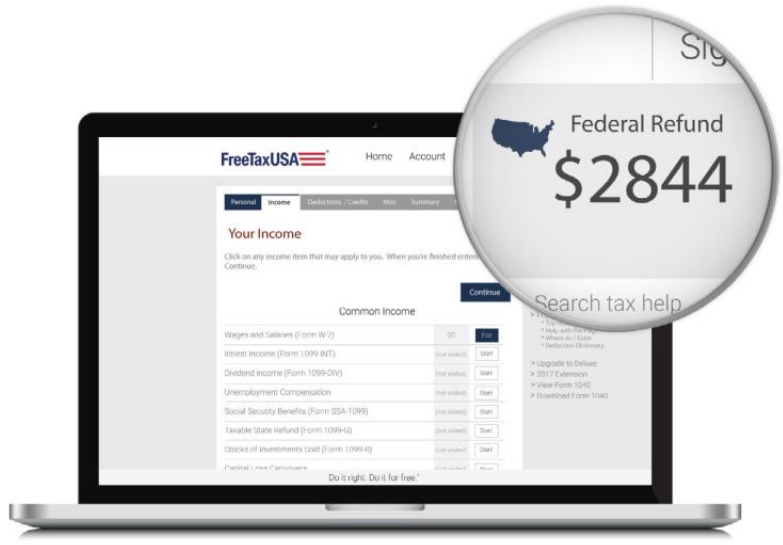
PROS: Good navigation tools, user interface, and IRS schedule support. Phone and chat help. Thorough review process. Price Lock guarantee.

CONS: Some help links lead directly to IRS documents. Expensive per-state filing.

BOTTOM LINE: TaxAct Online Plus features an excellent user interface, navigation, and help tools. Furthermore, its low federal e-filing cost makes it one of the best values among tax preparation services this year.

FreeTax USA Deluxe 2018 (Tax Year 2017)

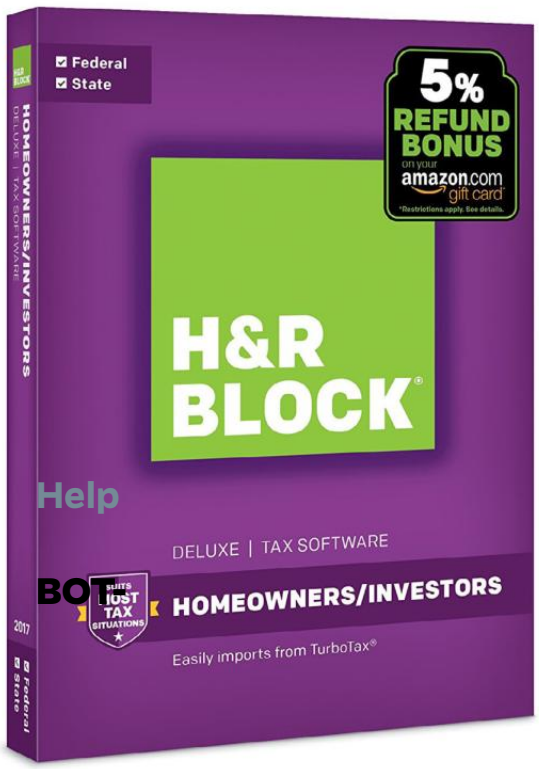
$6.99



PROS: Fast. Free federal e-filing. Inexpensive state filing. Comprehensive site outline. Flexible navigation. Ubiquitous context-sensitive help.

CONS: No comprehensive interview option. No Life Events feature. Can't import W-2s, 1099s.

BOTTOM LINE: FreeTax USA is a robust personal tax preparation website that lets you e-file your federal tax returns for free, though you have to pay for state filing and support.



H&R Block Deluxe 2018 (Tax Year 2017)

$54.99

PROS: Clean user interface. Clear navigation. Comprehensive coverage of tax topics. Accessible help. Data import of W-2 and 1099s.

CONS: No Life Events feature. Some nonstandard navigation. is lacking in some areas. Lacks linear navigation wizard.

BOTTOM LINE: H&R Block Deluxe is a highly capable and well-designed tax prep service that helps users claim relevant deductions and credits. It can be tricky to navigate, though, and help can be spotty.

Credit Karma Tax 2018 (Tax Year 2017)

Free

PROS: Free. Supports all major IRS and state forms and schedules. Clean, simple interface.

CONS: Insufficient, spotty help. Missing two state returns and some forms/situations. Search tool not always accurate. No overall site navigation tool.

BOTTOM LINE: The completely free Credit Karma Tax supports all major IRS forms and schedules for federal and state returns, but it has an atypical navigation system, anemic help resources, and it doesn't yet offer returns for every state.

Liberty Tax Online Basic 2018 (Tax Year 2017)

$24.95

●●●○○

PROS: Clean, simple user experience. Innovative navigation pane. Excellent review process.

CONS: Expensive state returns. Lacks linear walk-through option. No hyperlinked terms in Q&A or consistent context-sensitive help.

BOTTOM LINE: Liberty Tax Online Basic is a decent service from the well-known brick-and-mortar tax preparers. It's easy enough to use but lacks well-integrated, accessible guidance.

TaxSlayer Classic 2018 (Tax Year 2017)

$17.00

●●●○○

PROS: Inexpensive. Supports all major IRS forms and schedules. W-2 import from providers. Email and phone help. Good knowledge base.

CONS: Could use more and better context-sensitive help. User experience needs refinement. Tax return review not effective in testing. No Life Events feature.

BOTTOM LINE: TaxSlayer Classic is an affordable tax preparation service, but its context-sensitive help is lacking and its user interface could use more polish.

Jackson Hewitt Deluxe 2018 (Tax Year 2017)

$69.95

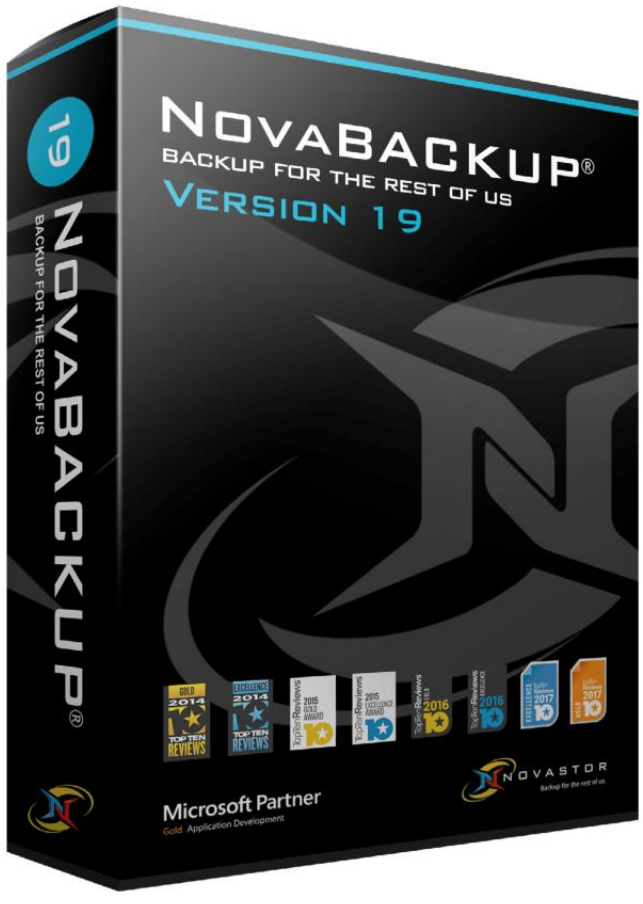
●●○○○

PROS: Comprehensive coverage of tax topics. Improved review process.

CONS: Pricey. Frustrating UI and navigation. Amount and quality of context-sensitive help is lacking. Can't import data from competitors or previous Jackson Hewitt filings.

BOTTOM LINE: The user experience, navigation tools, and help system you get with Jackson Hewitt Deluxe aren't up to par, especially given its high price. There are better ways to file your taxes online.

KATHY YAKAL



NovaBackup PC: A Solid Local Backup Solution

NovaBackup PC

Starts at $49.95 per year

●●●◐○

Local backup software creates redundant copies of your files on local media devices. These extra copies can come in handy if you accidentally delete something or your PC falls victim to a malicious attack. It's also a good idea to have multiple devices with the same backups in case disaster strikes twice.

NovaBackup PC can help you with your backup needs, including creating full disk images or network drive copies, and offers good security and customization options at a reasonable price. Its biggest shortcomings are an outdated interface and a lack of extras, such as File Explorer integration and ransomware protection. Still, these are not dealbreakers; NovaBackup does well enough to warrant your consideration.

PRICE AND PLATFORMS

NovaBackup PC costs $49.95 per year for a single license, $79.95 per year for a three pack, and $99.95 per year for five licenses. This subscription-based model is a departure from other local backup services, most of which require only a one-time purchase. This is not necessarily a drawback, though, since you receive all the updates to the software and premium US-based customer support.

The downside of this payment model is that you can't use it on as many computers as you want. Big-name corporations, such as Microsoft and Adobe, can get away with limiting the number of devices on which you can download and install subscription software, but this is a less feasible strategy in the crowded backup space. For the price of paying a subscription, NovaBackup needs to offer differentiating features. You can test out NovaBackup via a free trial version.

For comparison, Editors' Choice Acronis True Image costs $49.99 for a single, standalone license, with upgrade options starting at $29.99. But Acronis' $49.99 per year subscription tier gets you everything in the local-only software plus 250GB of cloud storage. Paragon Backup and Recovery costs just $29.95 for a perpetual license.

NovaBackup works on PCs as far back as Windows 7 SP1 and up to the latest release of Windows 10. NovaBackup does not offer any software for macOS, iOS, or Android devices. Apps for any of these platforms, or even a web interface, could be useful for running backup processes remotely. That said, it does offer solutions for Linux devices and servers.

NovaBackup PC

PROS Solid security. Highly customizable. Fast backups. Unlimited file versions retention. Can create disk images.

CONS Cluttered interface. Annual subscription model. No Mac support. Lacks File Explorer integration.

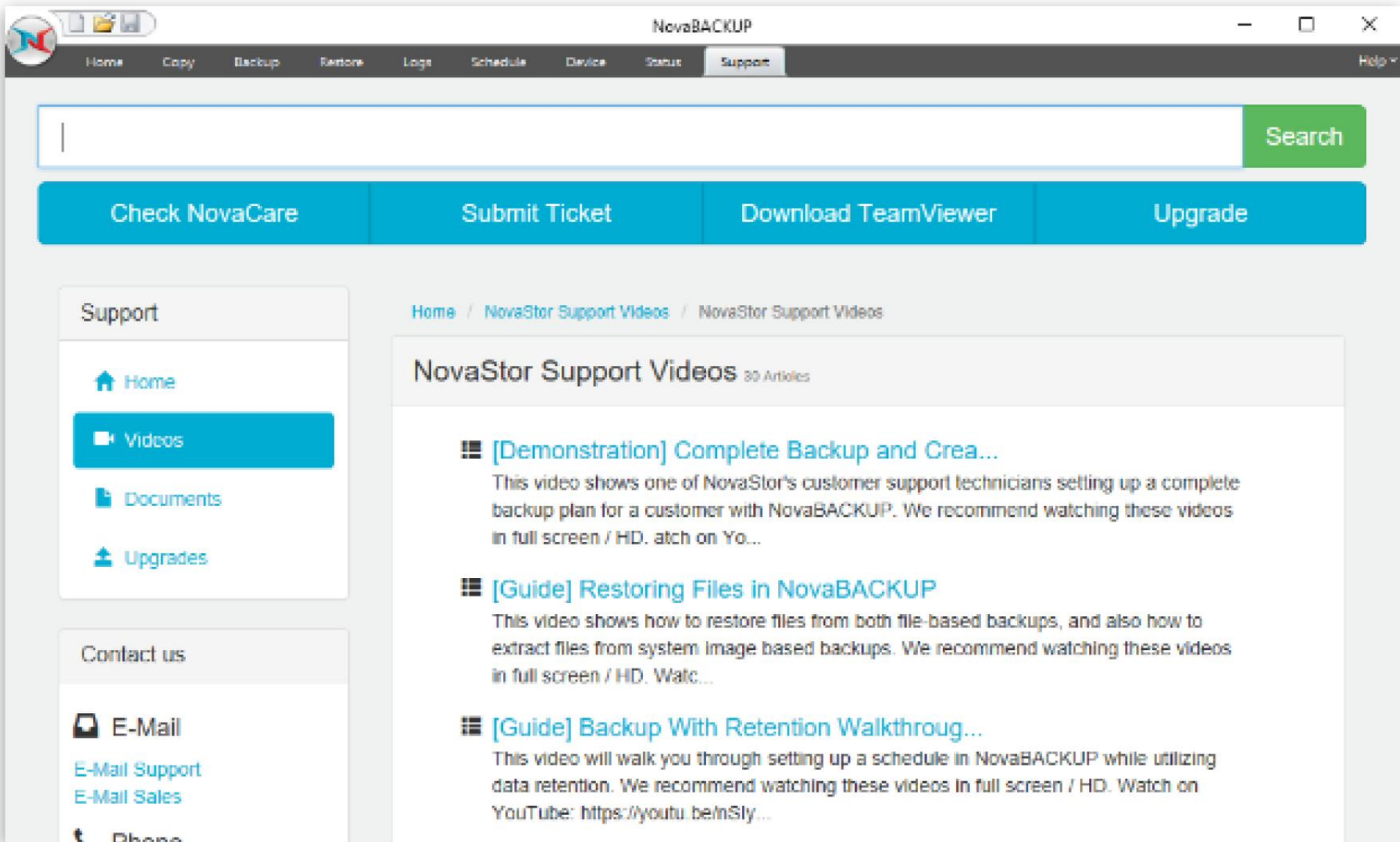
GETTING STARTED AND SECURITY

During setup, NovaBackup PC requires you to enter a name and a valid email address, but this doesn't create an account. The installer file is pretty lightweight at 247MB, and the entire installation process took less than 10 minutes on my test PC, a Lenovo ThinkPad T470 with an Intel i5-7300U and 16GB RAM running 64-bit Windows 10 Pro.

Once the installation is complete, you see the main desktop interface. Advanced users can dive right into configuring their backup sets, but newcomers should head to the Support tab, where NovaBackup PC hosts tutorial videos and general help topics.

One of NovaBackup's strong point is its security. As a fully local backup software, it does not connect to the internet at all and never uploads files to a server. In terms of file encryption, NovaBackup offers up to AES-256 encryption and hashes out your encryption key for maximum security. But it doesn't have higher-end features such as Acronis' ransomware scanner.

> **As a fully local backup software, it does not connect to the internet at all and never uploads files to a server.**

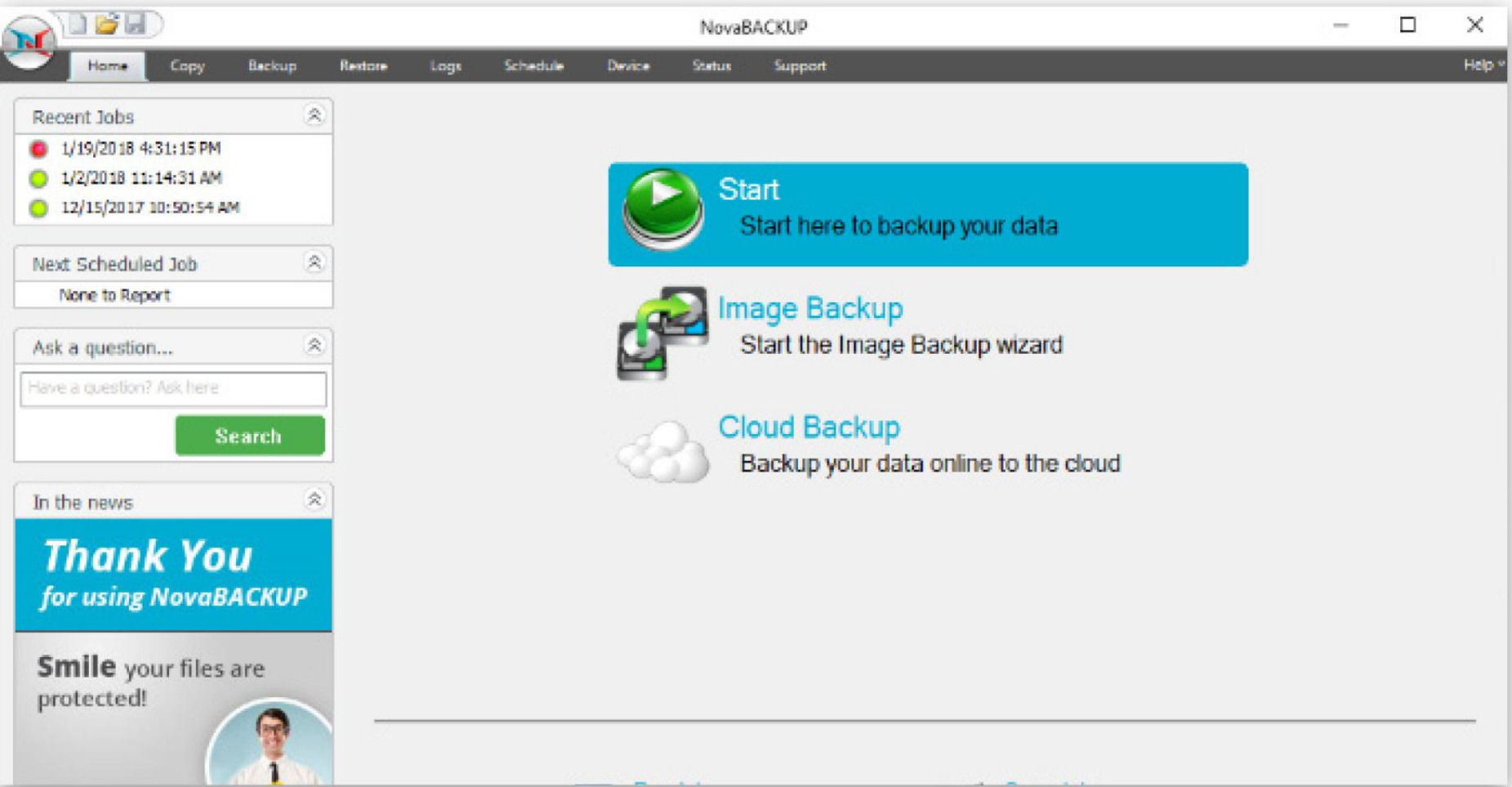


DESKTOP INTERFACE

The grey desktop interface feels crowded, with dated iconography and Windows Vista–style tabs. Although people familiar with backup software will be able to navigate well enough, this setup might confuse those new to the process. There's no clear flow to the experience, though most people will figure out that they need to click the large Start button in the middle of the Home tab. Competitor Paragon Backup and Recovery looks significantly cleaner and has a more compelling layout.

On the left-hand panel, you can view any recent or scheduled jobs, which helps improve usability. That said, the Ask a Question and In the News sections directly below those links look like ads. On the bottom of the home page are four links for running a job, opening a job, importing media, and adding a network drive. Nine tabs run across the top—Home, Copy, Backup, Restore, Logs, Schedule, Device, Status, and Support. These sections use a basic but effective file browser for selecting and viewing your local files.

NovaBackup's notification tray icon lets you start, pause or restart the backup service, but I wish this had a few more quick-action options, such as a link to the status of the backup or even to the program settings. File Explorer integration is another feature that I would like to see added. Although it is easy enough to select files to back up within the interface itself, it's more convenient to add files and folders to a set straight from the source.



MAIN FEATURES

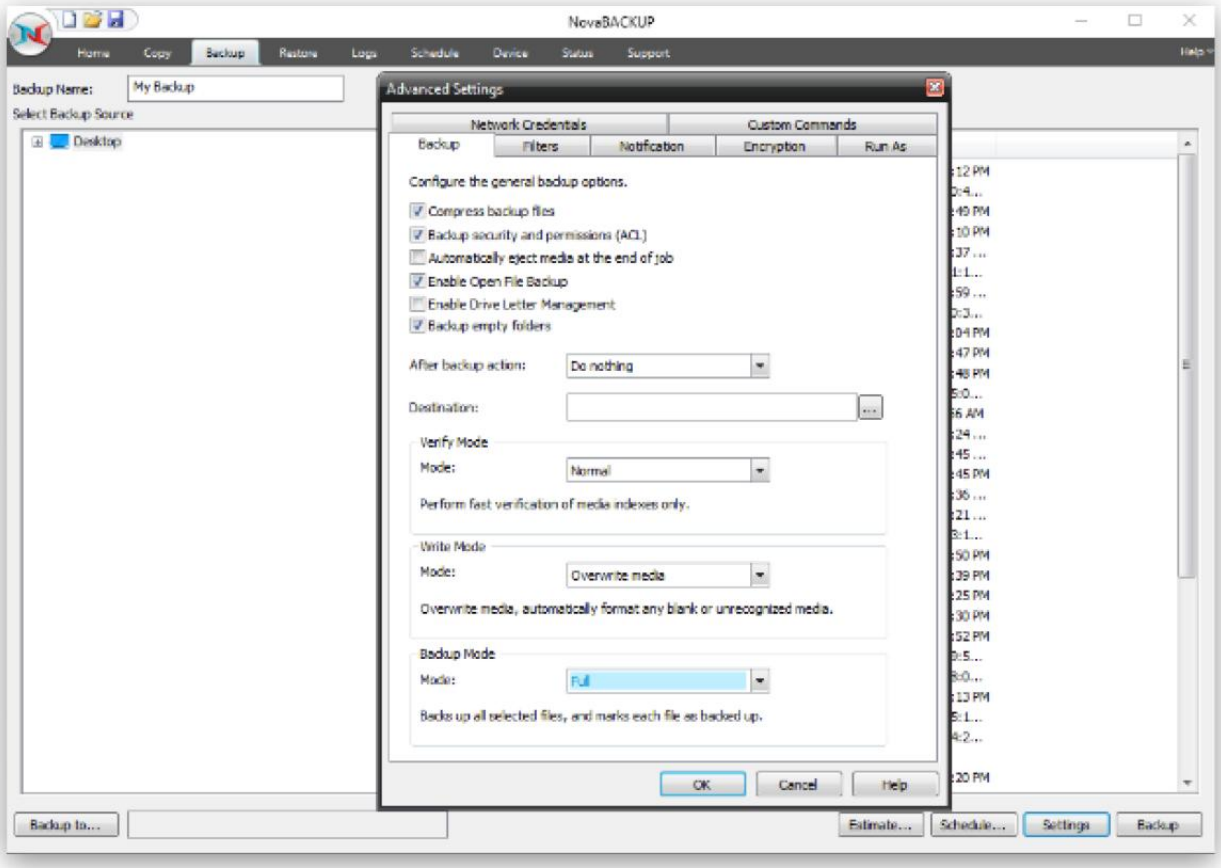
Like most other local backup software, NovaBackup requires you to configure individual backup jobs. NovaBackup does not impose any limits on what you can back up; system files, full disk images, and network drives are all fair game. The program gives you several options for scheduling your backup, including One Time, Minute, Hourly, Daily, Weekly, and Monthly. You also can set it to sync folders or files continuously with a connected cloud backup service such as OneDrive or Dropbox, even though this is not its primary use case. Those services, of course, have their own solutions for backing up your data to the cloud.

To clarify, NovaBackup does not offer online storage with its subscription. Instead, it requires you to set up a connection with an existing file syncing service as the destination for your backups. The other option is to use cloud storage site FirstBackup, which Novastor says is a preferred partner. The FirstBackup website looks sketchy, and even worse, its data storage prices are comically high. For example, it charges $89.99 per month or a slightly discounted $1,000 a year for 100GB of storage. For 1TB of data (half of the storage IDrive offers for $69.50), you need to pay a ridiculous $5,499 sum per year, roughly equivalent to your annual IRA contribution limits. Adding other computers to your account costs an extra $25 per year.

Since NovaStor does not bill itself as an online backup solution, this doesn't count against its score. But since the cloud backup option appears as prominently as the local backup option in the software itself, the steep prices are aggravating.

CONFIGURE YOUR BACKUP

NovaBackup gives you a few different options for verifying, writing, and ultimately backing up your files. Starting with Verify modes, you can choose between None, Normal, and Advanced. It's important to switch this setting on to ensure that the backup completes successfully. For Write modes, you can either choose to overwrite media or append to media, depending on whether you want to keep the original files on your hard drive. Multiple Backup modes include Full and Snapshot; both back up all the files you selected, but only the former marks each file as backed up. Incremental and Differential both look at which files have changed since the last backup job ran, but only the former marks each file as backed up.



Rounding out the backup preferences are the options to set up backup completion notifications, filter out certain files from the backup, and configure custom commands to run before or after the backup process completes, such as ejecting media or restarting the computer.

> **Since the cloud backup option appears as prominently as the local backup option, the steep prices are aggravating.**

BACKUP PERFORMANCE

I tested NovaBackup's performance by backing up a 15GB folder with mixed-media file types on a Lenovo ThinkPad T470 to an external drive. NovaBackup completed the test in a rapid 2:18 (minutes:seconds), and that's with AES 256-bit encryption enabled. One complaint I have about the status window of the backup is that the time and bytes estimates are a bit jumpy, though they do offer a good amount of detail.

For comparison, I tested all the other local backup services in our roundup with the same file collection and on the same system. Acronis True Image bested NovaBackup, completing the test in a blazing-fast 1:35 with AES 256-bit encryption enabled. Other services came in with slower times, but not by much. NTI Backup Pro notably took 17:04 for the same task.

RESTORING FILES

NovaBackup can save an unlimited number of file versions. The only limit is the amount of storage you have at your disposal on your backup destination. To access other versions of a file, go to the Restore Tab and access the program's Time Mode.

From the Restore tab, there are two modes to choose between, Time Mode and Device Mode. Device Mode should be familiar to most users; here, you can select from any of your backup sets. NovaBackup keeps files in their original structure, so you can restore everything as is or select individual files and folders. The Time Mode adds a slider that lets you view a history of your backup jobs and select ones to restore within a specific time frame. In testing, I successfully restored older versions of backed-up files using this selection mode.

As with the Backup tab, you get a ton of settings to configure. For example, you can set up filters, choose how to deal with existing files, and even set up some commands to run after the restore operation completes. Further options let you specify which accounts should be used to run a particular job.

A SOLID CHOICE

When you have important data on your computer, you need to have some sort of backup process in place. NovaBackup PC is a good option. It's fast and highly customizable, and it has solid security features. That said, its biggest downsides are an outdated interface and the lack of Mac support. Further, the subscription model feels limited, since software such as Acronis, our top pick, offers comparable local backup options, online backup capabilities, cross-platform support, and ransomware protection for the same price per year all wrapped in an excellent interface.

BEN MOORE

What Is Cyber Insurance, and Do You Need It?

BY ROB MARVIN

The internet is a dangerous place to depend on when it comes to your business, finances, or livelihood in general. Yet in our hyper-connected world, we all rely on it more than we would like. We give our data to companies and services. We pay bills and buy things online. We put our entire identities on the web, do our best to protect our identities and secure our data, and cross our fingers that the next massive data breach won't affect any of the services we've trusted with valued personal or financial information.

“Your data can be compromised by a service you didn’t even know had your personally identifiable information (PII).”

And security isn't getting any easier: Our digital landscape is rife with phishing; all kinds of malware, including ransomware; brute-force botnets perpetrating massive DDoS attacks; and plenty more nasty hacks and potential attack vectors. Cybercriminals are getting smarter and are already beginning to use artificial intelligence (AI) and machine learning (ML) to more effectively target businesses and individuals.

As the Equifax breach taught virtually every adult in the United States, sometimes your data can be compromised by a service you didn't even know had your personally identifiable information (PII). The recently disclosed Meltdown and Spectre vulnerabilities serve as yet another reminder that your computers and smart devices may be compromised without you even knowing it. At this point, there's no guarantee that any of your data is 100 percent safe.

What you can do, either as a business or an individual, is to cover potential losses with cyber insurance. There are plenty of benefits and drawbacks to buying cyber-liability coverage (which we'll get into below), but if you already have insurance policies for your house, car, health, pet, and life, why not cover your online data and digital identity as well?

WHAT IS CYBER INSURANCE?

Cyber insurance has been around for more than a decade. Market research firm Progressive Markets projects the global cyber insurance market to hit more than $29 billion by 2025, while PwC estimates it will reach $7.5 billion as soon as 2020.

Cyber insurance is a subcategory of general insurance that covers businesses and individuals against internet-based liability and risks. There are generally two levels of cyber liability coverage: first-party and third-party. First-party coverage encompasses direct losses to an organization or individual, whereas third-party coverage extends to claims and legal action taken by customers or partners.

Coverage differs by provider, but common coverage areas include data breaches, identity theft, and personal data theft. There are also the hefty legal fees, fines, and costs associated with recovering compromised data, repairing systems, restoring the personal identities of affected customers, and notifying customers of breaches. Coverage may also extend to scenarios like business interruption, extortion, or forensic investigation, meaning the costs associated with uncovering the cause and impact of an attack. The core idea behind cyber insurance is to help you recover from a data breach or identity theft by mitigating all the costs that crop up in the aftermath.

BUSINESS OR PERSONAL

It's important to distinguish between cyber insurance policies aimed at individuals and those covering an entire company. Most providers cater more toward business policies, but a number also offer personal plans, which are primarily focused on identity theft coverage: This means factors such as income protection and expense reimbursement associated with recovering your identity, restoring your credit history, and legal action against identity thieves. Other personal cyber insurance plans can extend to issues like computer virus coverage or physical computer damage.

Most providers cater more toward business policies, but a number also offer personal plans.

For businesses, cyber insurance policies can get a lot more complicated. Plans range from those catering to small to midsize businesses (SMBs) to coverage for large corporations and enterprises. Coverage starts with the data you collect and store on customers, be it credit card of bank account numbers, Social Security or driver's license numbers, or simply addresses and phone numbers. A basic coverage plan for a smaller business might cover breach notifications, credit and fraud monitoring services, the costs associated with hiring a PR firm, and the cost of restoring and recreating data.

Corporate cyber liability plans have heavier duty coverage. Beyond risk management for data loss mitigation and prevention, incident response, as well as third-party legal and regulatory costs, this means the policies need to scale. This is particularly important when it comes to data breach notifications in the wake of scandals like Uber's 2016 breach, which it waited to disclose for a year. This led the US Senate to introduce the Data Security and Breach Notification Act, which would require companies to report data breaches within 30 days. The requirements are even more stringent for businesses operating in Europe, where the General Data Protection Regulation (GDPR) going into effect this year requires customer notification within 72 hours.

HOW TO GET COVERAGE

There's a whole laundry list of cyber insurance plans offered by traditional providers and security-specific companies. Here's a breakdown of some of the most popular plans and providers and what the liability coverage entails:

ABA INSURANCE: First- and third-party coverage protecting businesses from computer, network, and internet-based risks.

AIG: According to credit rating agency Fitch's latest "Cyber Insurance Market Share and Performance" report, insurance giant AIG is one of the top three cyber insurers on the market. AIG offers a number of different cyber insurance plans including personal identity coverage and its CyberEdge plan for businesses covering first- and third-party recovery, loss prevention, extortion, and more. There's also a CyberEdge Plus plan that covers bodily injury or property damage associated with a cyberattack, as well as business interruption costs and product liability.

AXIS CAPITAL: Business cyber liability coverage including not only the basics—data breaches, extortion and loss, data recovery, third-party defense, etc—but also factors such as intellectual property infringement, employee fraud, DDoS attacks, and introduction of malicious code into a company's system.

BCS: BCS Insurance offers cyber and privacy loss protection plans through Blue Cross and Blue Shield for data and network breaches, data loss caused by an outsourcer or vendor, and third-party legal protection plus administrative features overseeing breach notifications and incident response.

CHUBB: Another top insurer according to Fitch, Chubb offers a wide array of cyber insurance products and services including loss mitigation and incident response, and customizable risk management policies covering privacy, network breaches, media, and claims related to errors and omissions.

CNA: CNA's NetProtect Cyber Liability insurance covers first- and third-party factors including network extortion, business interruption expenses, electronic theft, and liability pertaining to media, privacy, network security, and breach notification laws and defense.

DATA BREACH INSURANCE: This provider's CyberCruiseControl process encompasses cyber threat identification, protection, control, and a number of insurance policies such as breach, cybercrime, and intellectual property insurance.

INSUREON: Small business insurer Insureon offers a wide array of cyber liability insurance covering both first-party response and third-party defense.

LIBERTY MUTUAL: Offers identity fraud expense coverage as well as data theft and cyber coverage add-ons to its general liability insurance for business owners.

NATIONWIDE: Nationwide offers three cyber insurance plans: data compromise protection, identify theft protection, and its CyberOne protection plan. CyberOne covers full data restoration and recreation, lost business expenses, plus data breach notifications and damaged system repairs.

RSA BROKER: Not to be confused with the security conference, RSA Broker offers a cyber risk policy covering 24/7 incident response, IT forensics, PR and legal advice, defense costs and penalties, extortion, business interruption, and data loss and liability for businesses.

TRAVELERS: Travelers Insurance offers a number of different plans and related services. The plans include a CyberEssentials package for SMBs, CyberFirst plans for tech companies and public entities, and CyberRisk plans for larger businesses. The insurer also has so-called "cyber coaches" plus an online academy and risk hub, and offers pre-breach services such as assessments and training through a partnership with Symantec.

XL GROUP: XL's cyber and technology insurance covers privacy and security liability, data breach response and crisis management, business interruption expenses, data recovery costs, cyber extortion, and any fines and penalties from legal or regulatory action.

BUYING FACTORS TO CONSIDER

There are a host of factors to consider when buying a policy. Whether you go through a broker or buy direct from an insurance provider, cyber insurance is like any other coverage: there are plenty of hidden fees and conditions to be aware of before you lock yourself into a contract.

A good starting point is a cyber insurance buyers' guide. It's important to know when your coverage will trigger and when it won't (for instance most plans don't cover terrorism-related cyberattacks), whether the plan suits your specific data risk and coverage needs, and what claims are excluded.

Insurers also go through a detailed underwriting process to evaluate the risk and potential exposure of customers. For businesses in particular, it's important to do your due diligence beforehand and get your security ducks in a row. Does your company have a CISO? What security software and incident response systems do you have in place? What types of customer data are you collecting and how are you encrypting and protecting it? Cyber insurance premiums can get quite pricey, and will be even more expensive the more risk factors you have. Check out this cyber insurance premium calculator for a rough estimate depending on your business type and size, or you can request a quote from a provider directly.

“There are plenty of hidden fees and conditions to be aware of before you lock yourself into a contract.”

IS IT WORTHWHILE?

One key fact to remember is that cyber insurance is not a replacement for cybersecurity—it's not a tech solution. Cyber insurance coverage is your personal or professional fail-safe should a breach or cyber attack occur, and you're left with mountain of costs to restore your business, deal with customer lawsuits, or reclaim your digital and financial identity.

You should still have a comprehensive suite of security tools in place, including antivirus and ransomware protection as well as encryption software. And don't forget about password managers and two-factor authentication (2FA) to protect against identity theft.

As for whether buying cyber insurance is worthwhile, it comes down to peace of mind. Do potentially high premiums for insurance you may not need offset the risk of having your identity stolen or your company's infrastructure breached and data stolen? If you choose the right policy that protects exactly the coverage areas and attack vectors you need, it may be worth the money as cybersecurity incidents increase in frequency and severity across the web.

It's also worth asking whether insurers can even afford the skyrocketing risk. As breaches and identity thefts continue and providers are saddled with the cleanup costs, is cyber insurance yet another bubble waiting to burst?

ROB MARVIN

FITNESS TRACKERS CHANGED MY LIFE

BY VICTORIA SONG

My morning routine has an extra step now. Before I shower, I take off anywhere between one and six wearable devices. I hold out my arms and inspect the imprints they leave on my skin—long, angry, watch-shaped marks. When your bread and butter is reviewing fitness trackers, as I do for PCMag, I suppose you could say this is an occupational hazard.

It doesn't matter that wearables are increasingly becoming showerproof. Unless I'm testing how they hold up against water, I like to think there are at least fifteen minutes in a day when my body is not quantified.

These days, Fitbits and their ilk can track almost anything—from what time you go to bed to how quickly your heart beats when you're running to your next appointment. Some, like the Garmin Vivosmart 3, claim their algorithms can measure how stressed you are. Wear one tracker for a month, and you'll have a decent chunk of data that says something about who you are.

But the same questions about wearables have persisted since the technology first debuted: Does this data actually help you in any way? Is your fitness tracker a useful tool on your path to wellness or just tech-justified navel gazing? Opinions and study results range widely, and we still have no definitive answers.

But in my first year of testing them, wearables have had some unexpected effects on me—some vaguely negative, some neutral, and a couple positive experiences that made me rethink my life. My year in wearables might not answer any of the big questions, but it might offer some insight into the future potential these gadgets contain.

THE IDEAL OF THE QUANTIFIED SELF

How well do you know yourself?

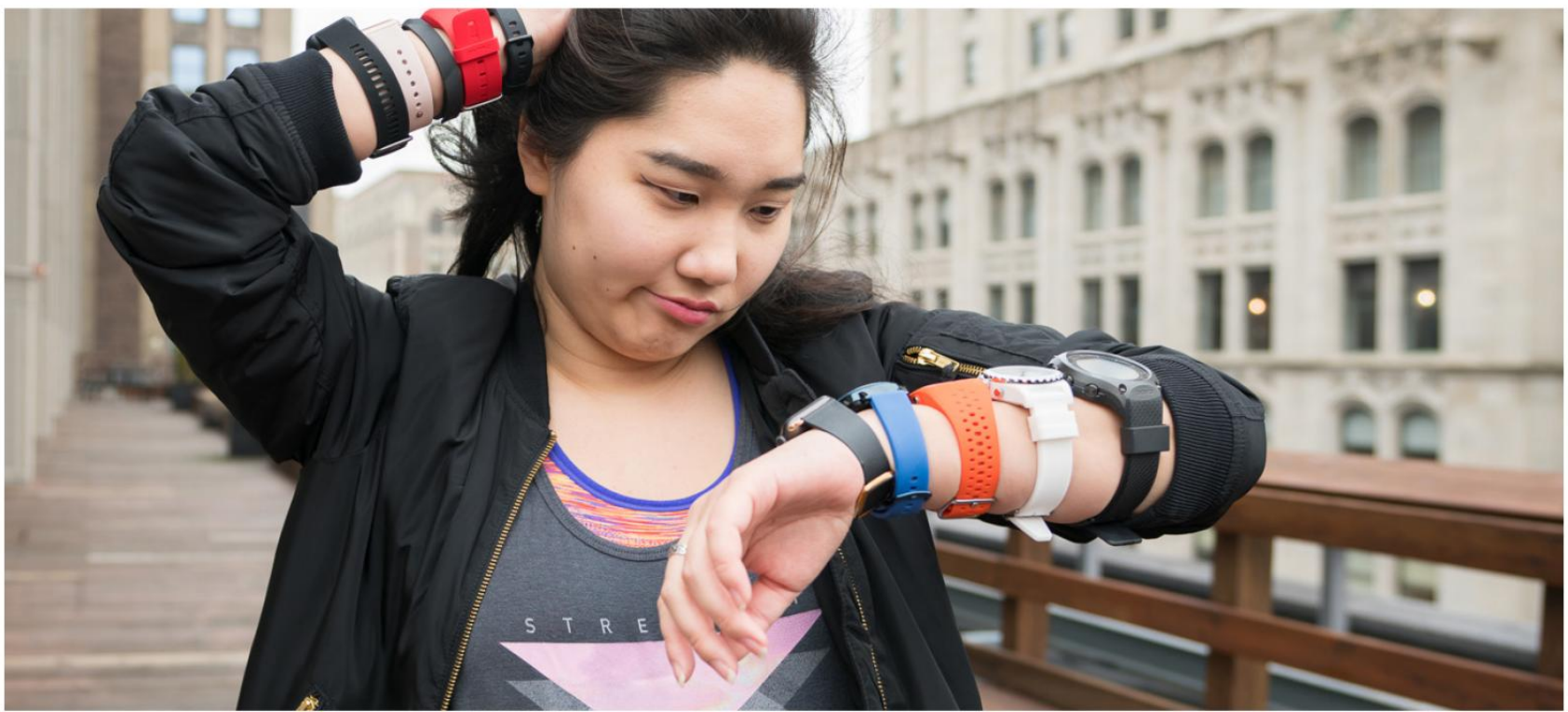
I'm not talking about your identity, values, or opinion on whether a hamburger qualifies as a sandwich. I'm not even talking about your weight, height, or eye color. I mean things like this: In the last 30-day period, how many hours of sleep did you get each night, on average? If the nearest train station is two miles on foot, at your average pace, how many steps do you think you'll take to get there? When you're sitting at your desk, what's your resting heart rate?

In the last 30 days, my Fitbit Alta HR tells me, I slept an abysmal average of 5 hours and 45 minutes per night. I walk at an average pace of 3.5 miles per hour, which means it takes me about 34 minutes to walk 2 miles. For me, a 5-foot 3-inch woman, that's somewhere between 4,000 and 4,200 steps. When I sit at my desk (depending on how stressed I am about an upcoming deadline), my resting heart rate is about 80 beats per minute. It drops down to around 50 beats per minute when I sleep, for an overall daily average of 68 to 70 bpm. I'm less consistent with my steps; some weeks I'll go as high as 100,000 in a week. But generally I take somewhere between 50,000 and 70,000.

So what's the point of knowing all that?

Supposedly, it's meant to make you aware, or, if you like buzzwords, mindful. The data paints one kind of picture of who you are. The positive potential for collecting all this data isn't hard to imagine—medical use cases, weight loss, changing bad habits like lazing on the couch with a bag of Cheetos. That's the promise you're buying into when you invest in a fitness tracker. Every buzz and achievement badge you unlock is meant to motivate you to change your behavior for the better.

Scientifically, the jury is out as to whether wearables actually help to change behavioral habits. For every study that says wearables have no impact on improving health, you can find one that says they do—albeit a moderate effect. A 2015 review of wearable studies by the Department of Veteran Affairs concluded that they had "small positive effects on physical activity and weight." And a 2016 Gartner survey found that the abandonment rate for fitness trackers was 30 percent, as users didn't find them particularly useful or got bored.

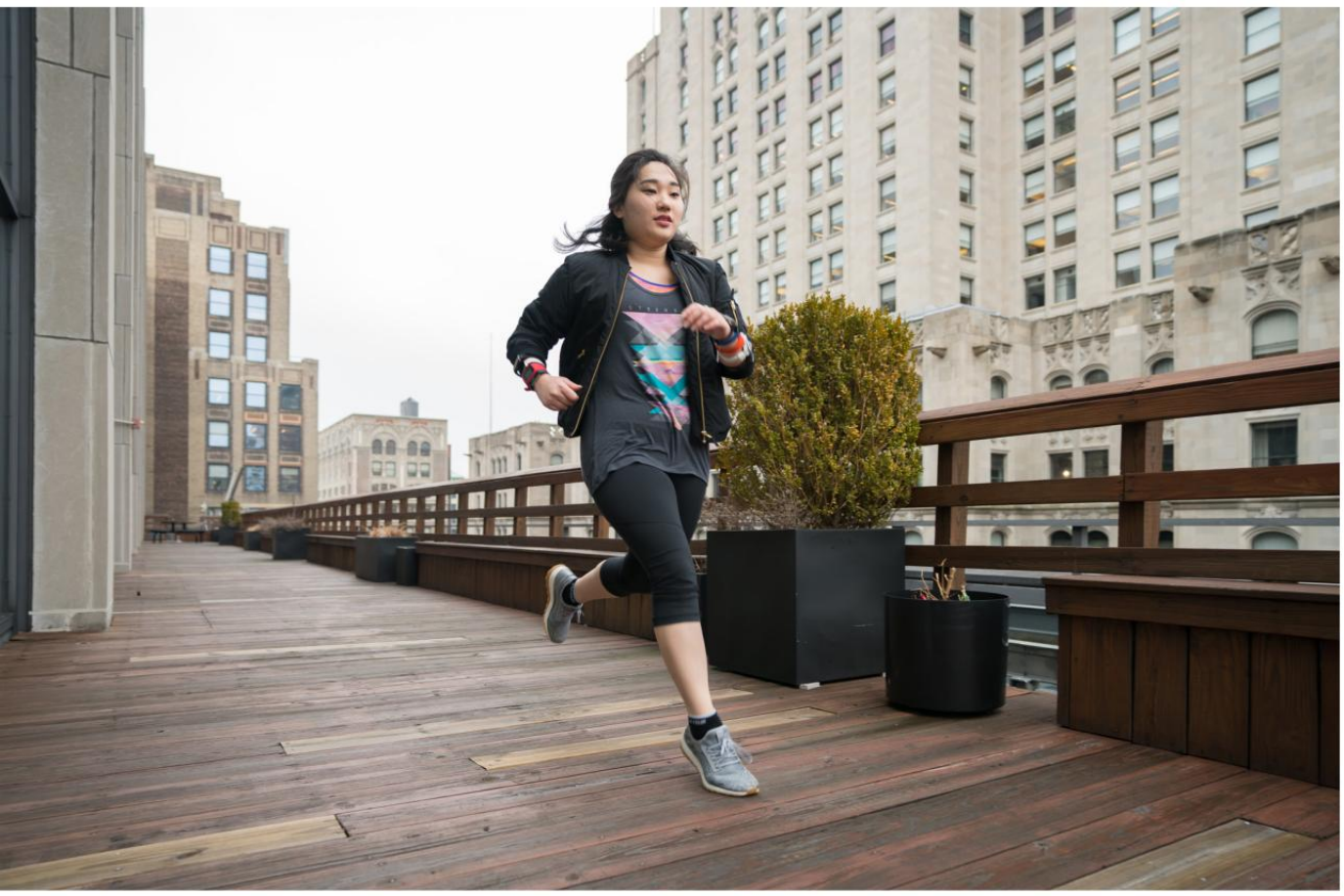


“Many people are excited by the opportunity [to change health behaviors]. But that’s part of the challenge. For most people, for the average person, and especially someone who has a chronic condition or is overweight, giving someone a wearable device is not effective at improving their behavior,” says Mitesh Patel, Assistant Professor of Health Care Management at The Wharton School, University of Pennsylvania.

But when you ask a wearables maker, they’re going to tell you differently. After all, they spend a lot of time, money, and effort on designing products and apps that retain and motivate users.

It had a rocky start last year, but to the average consumer, Fitbit is consistently one of the top wearables brands. In 2017, the company reported that its active user base grew to more than 25 million. “From our perspective,” says Melanie Chase, VP of product marketing at Fitbit, “we want to be a wearable that people wear all the time. And then on top of that, there are real motivating features that keep people moving.”

> **I found reasons to get up—mostly to trek to the water cooler in the office pantry, exactly 220 steps from my desk.**



Of these features, Chase points to Fitbit's Reminders to Move: 10 minutes before each hour, you get a buzz on your arm encouraging you to take 250 steps. I've become intimately familiar with this feature; at one point, I wouldn't even need to look down at my wrist to know it was ten to the hour. In the beginning I'd comply, especially if I felt like productively procrastinating. Later, it just gets easy to ignore.

"Our team here, which has behavior change experts and research scientists, modeled out a bunch of ways to deliver this feature," says Chase. "What we found was if you buzz people ten minutes before, they had time to make an impact. Then, you buzz them to reward them afterwards. We've seen 70 percent of our low-activity users moved more after using our reminders, and then even beyond that, months later, we were seeing changes in their patterns."

It's hard to argue the numbers when you don't have access to Fitbit's vault of data. But in my own experience, at least in the beginning, it worked. I found reasons to get up from my desk—mostly to trek to the water cooler in the office pantry, exactly 220 steps from my desk—so I could hit my goal.

I can also tell you that after a few months, I went into the app and disabled it—because it drove me crazy.

YOU'RE YOUR OWN WORST ENEMY

It's no secret that many fitness trackers end up collecting dust at the bottom of a drawer after a few months. Humans are notoriously good at keeping bad habits and bad at building good ones.

It doesn't help that finding a wearable that works just right for you is hard to do. Whether they're on your wrist, in your ears, or clinging to the underside of your bra, no one really agrees on what's the best way to make them stick. Either they're too bulky, too uncomfortable, or you just get tired of the whole routine. In fact, when you get a bunch of wearables reviewers together, we whisper about those glorious days when you don't have to wear one at all; when your wrists are bare, you don't have to deal with the anxiety of failing to reach your daily step goal or count the days since you've crushed it at the gym. (Hint: It's always too many.)

When you get a bunch of wearables reviewers together, we whisper about those glorious days when you don't have to wear one at all.

Though the stickiness problem is a many-headed hydra, battery life definitely plays a big role. In reviews, it can be the deciding factor between an Editors' Choice or a middle-of-the-line 3-star rating. Take the Fitbit Ionic: According to Chase, every Fitbit product is rated for 5-plus days of battery life—and in testing, I found the Ionic lasted as long as a full week without needing a charge. Conversely, the Apple Watch Series 3 with LTE zapped out after just a day and a half in regular use.

Charging is relatively simple, but a wearable isn't like a smartphone. The average person can safely leave a fitness tracker at home without consequences, other than losing a day of data. But when one day turns into two days turns into two months, the stickiness is gone.

"Every time you take off the device, there's a chance you're not going to put it back on," says Patel. "Any device you have to take off when you go in the shower or you have charge every couple of days, people are less likely to stick with that, because they have to actively put it back on."

Another problem lies in how these devices provide incentives. Leaderboards are a popular feature in many wearable apps. The idea is that competing against your peers will inspire you to get up off that couch.

“It’s no secret that many fitness trackers end up collecting dust at the bottom of a drawer after a few months.”

“The leaderboard is a big motivator. Throughout Fitbit’s history, people with at least one friend take 700 more steps per day than people who don’t have friends,” says Chase. “You can throw out a challenge [against your friends], and what we see is that people take 2,000 more steps per day when they participate in a challenge.”

Whether that works, though, depends on your personality. For a couple weeks, I got into intense competitions with PCMag Senior Designer James Jacobsen that involved Sharks-versus-Jets finger snapping in the hallways, intensely sore feet, and weekly step counts surpassing 100,000. Bone tired after work and out of sheer spite, I’d drag my poor roommate and dog to Prospect Park for “Eff You James” walks to help me keep up or at least close the gap. But this kind of competitive fervor isn’t always sustainable. James won one week; I won the next. And then we stopped.

This kind of competitive fervor isn’t always sustainable. James won one week; I won the next. And then we stopped.

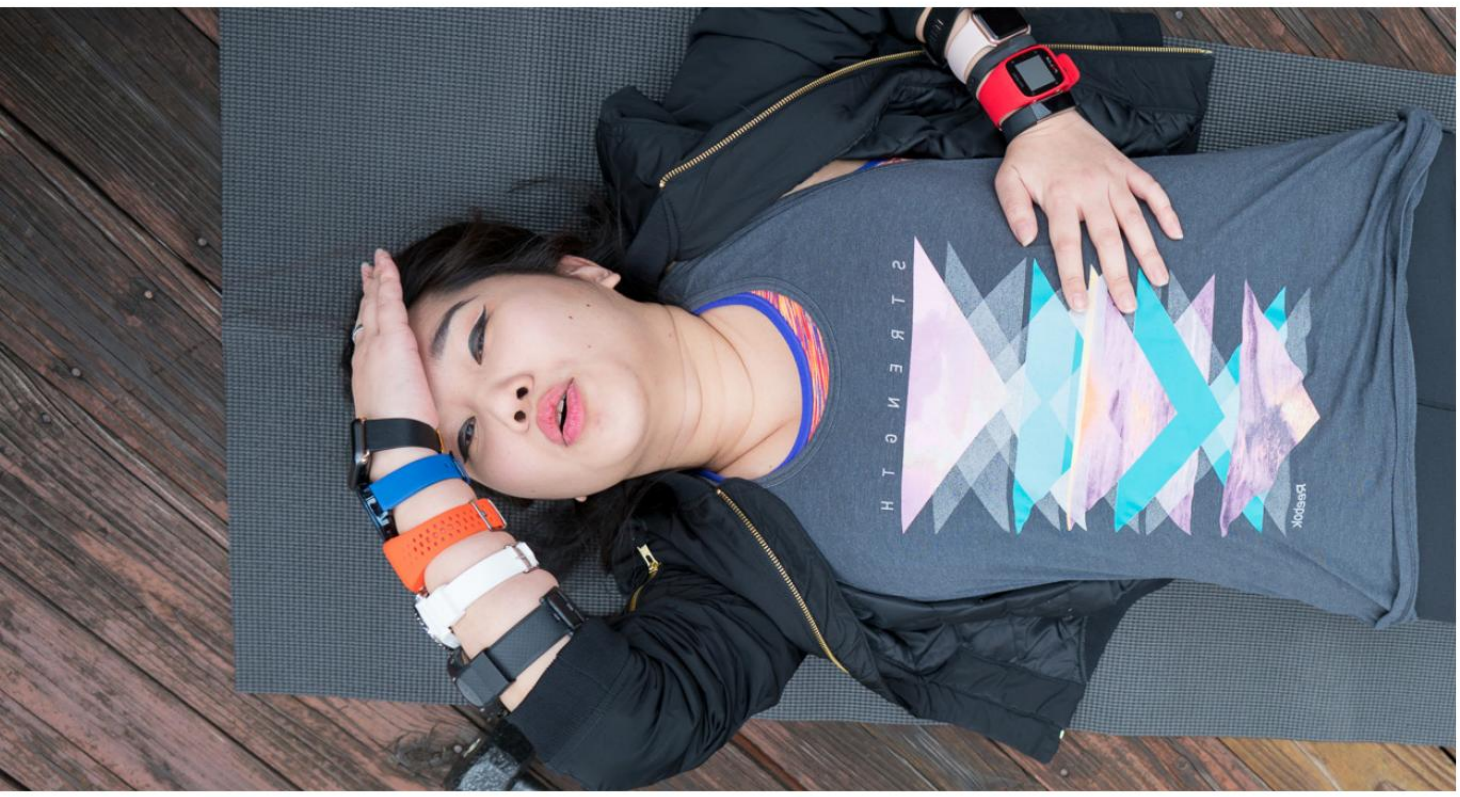
“The fundamental problem with the leaderboard is that it’s motivating the person at the top,” says Patel. “That person is already active to start. The people who need most motivation are the people at the bottom. However, they’re getting demotivated, because it’s hard to catch the person who is already going on a 5-mile run every day. We found it’s more effective to show them the person in the middle, because they’re shown something that’s within reach. The people who did the worst were the ones who got shown how top performers did.”

This bears out in practice, for me. When Fitbit launched the Ionic at a special event in Montauk this past August, the divide between fitness and tech journalists was like a high school cafeteria where jocks and nerds sit at different tables. Despite, shall we say, my lack of natural enthusiasm for physical exertion, I’m not totally unathletic. Growing up, I played softball, ran track (albeit slowly), played volleyball, swam, biked, skated, kickboxed, rock-climbed—the works.

But among the athletically endowed in Montauk, I was out of my league.

This was most evident during the two exercise events Fitbit had us participate in. In my hubris, I chose running and swimming—two activities I usually enjoy. The thing is, I enjoy them at my pace and ability. I can run 5K, around 3.1 miles, in about 45 minutes, and I have never claimed to be Speedy Gonzales. But running in a pack of buff fitness journalists led by ultramarathon runner Dean Karnazes is like trying to keep up with a modern-day Hermes. Fleet of foot and glistening, they glided atop the asphalt like lithe cheetahs. In comparison, I felt grossly inadequate, wheezing through a 4-mile course in blistering summer heat.

Doing a gator crawl with 20-pound weights at the bottom of a pool was like coming to terms with my own death by drowning.



Likewise, a pool exercise led by actual Amazon Gabby Reece left me mildly traumatized. I don’t have noodle arms, but doing a gator crawl with 20-pound weights at the bottom of a pool was like coming to terms with my own death by drowning. I am not ashamed that I couldn’t complete the grueling hour of exercise—I was actually flabbergasted that I made it through all but one of the circuits.

“It’s definitely not about shaming you,” Chase insists. “It’s not about, ‘Oh, you didn’t do a good job this time.’ It’s just about—get out there and try again.” But I was left wondering how many people of average or below-average fitness would feel when forced to face their own physical shortcomings—and whether it would put them off trying altogether.

NUMBERS MEAN NOTHING WITHOUT CONTEXT

In between testing lots of different wearables, I usually stick to the Fitbit Alta HR. It’s small enough to be unobtrusive, it’s flexibly fashionable, and its long battery life means I can get a decent amount of wear before I forget to charge it. I’ve been wearing the Alta HR for roughly a year, and because it’s my job, I’ve hooked it up to an If This Then That (IFTTT) recipe to automatically record my stats into a spreadsheet on my computer. I now have cells upon cells of personal data recorded by that device—how many steps I took on a given day, how many miles I walked, how many hours I slept.

It’s a diary of sorts—a record of my life in numbers. But there’s very little context for what I’m seeing. Take heart rate, for example. After a year, I have a pretty good sense of what my basic resting heart rate is. But that big picture only emerges after a long time. In the short term, it means hardly anything.

In early December, I was caught up in a gun scare at a movie theater in downtown Manhattan (it turned out to be a false alarm). I was wearing my Fitbit at the time. For me, this was a harrowing ordeal—I was trampled by a panicked crowd, lost my shoes, and ran barefoot into the freezing winter night. But these events registered only as spikes of sporadically elevated heart rate.

Because, again, I do this for a living, I checked my Fitbit mid-anxiety attack to see whether it could track the sudden change in my heart rate. As I hyperventilated on the sidewalk, I was impressed to see it had reached 110 bpm.

Later on, at home, even though I could see that my heart rate had rapidly jumped from 70 to 120 beats per minute, I found that it didn’t even register as light exercise in the app. I know I had an anxiety attack only because I remember the date, time, and circumstance. I have no idea how this data was parsed by Fitbit’s algorithm.

As someone with clinical depression and generalized anxiety disorder, managing anxiety and panic attacks is a part of my life. Regarding tracking my overall health and data, it'd be useful if I could get insight as to when these attacks occurred. That would give me a great incentive to stay on the wearable horse, so to speak. But unfortunately, insight into when these attacks might occur is not likely in the near term.

"When it comes to preventative care, doctors are not set up for that yet. There just isn't an infrastructure that's been built over time," says Dr. Steven LeBeouf, founder of Valencell, a biometric sensor technology company for wearables and "hearables" (trackers worn on or in your ears). "It'd have to be built by insurers, and they'd have to push it. On the prevention side, it's slow."

"Our goal is really to provide users with personalized guidance and actual insight based on their own data," adds Chase. "In terms of contextualizing the data we collect, we want to make it meaningful. We actually recently published a peer-reviewed paper that showed we were able to predict instances of atrial fibrillation about 98 percent of the time. But people aren't used to getting data from their Fitbit that says, 'Hey, you might have a heart condition, you should look into this.'"

People aren't used to getting data from their Fitbit that says, 'Hey, you might have a heart condition.'

Medically speaking, a lot of the marketing around heart-rate monitors centers on heart health. If you've seen one wearables press conference, you've seen them all—and usually, there's a story about how someone was able to detect a heart attack before it actually happened, because they noticed an abnormal spike in their bpm. That's a powerful narrative that speaks to the medical usefulness of wearables. But it's also limited to a certain demographic.

You'd think that more data might be the answer. But with metrics—heart rate, sleep, steps—there's only so much you can understand. And there's only so much that informs you about how your behaviors impact your health. After a few weeks, once you've established your baseline, the appeal of seeing how well you did each day wears off. Data fatigue is real.

"For most people, giving them more data is not helpful. It's about framing the data," says Patel.

"Data is so rich right now, in the sense that it's gotten so much more accurate, to the point where it could be really useful," adds LaBeouf. "But what we see a lot of people talking about today is well, we got these really accurate sensors. How can we provide more value to the consumer? It's less about the metrics and more about the new user experience."

THE HUMAN ELEMENT

For all the roadblocks and hurdles facing wearables to becoming more-concrete healthcare solutions, a greater awareness of your baseline can be incredibly valuable. Even if you're not a self-quantifying nut, the benefits of knowing your own body can't be discounted.

After my semi-active youth, I was not the type of person who imagined herself as a regular gym-goer or liable to run for anything other than the subway. So, of course, I found myself in my late twenties with some extra poundage. And because anyone who has ever dieted is intimately acquainted with calorie counting and the couch-to-5K program, I was ready to slough off some weight with the help of my handy-dandy Fitbit.

For a good 12 weeks, I laboriously logged every meal, calorie, and run, and hit my daily goal of 10,000 steps at least six days a week. I cut alcohol and desserts entirely from my diet, along with any food that was remotely delicious. I was subsisting on bland chicken, salmon, and steamed vegetables, and missing bread like it was the one true love of my life. I wasn't expecting to lose twenty pounds in a month, but I should have seen some progress in exchange for my sacrifices. Instead, I gained weight. And not in muscle.

Surely, I thought, the universe couldn't hate me that much. So I visited my doctor and relayed my frustrations. I didn't go so far as to whip out my phone and wave the data in my doctor's face, but it did provide evidence that my weight gain continued despite a strict diet and exercise plan.

Blood tests later revealed that my high testosterone levels and infrequent periods made it likely I had polycystic ovary syndrome—a condition that often leads to weight gain in women. I'd never thought twice before about whether something other than poor lifestyle choices could be a factor in my struggle to lose weight. I'm not entirely sure I would've found out if I hadn't bought a fitness tracker.

Experts say that certain psychological tricks could determine whether wearables evolve into an essential piece of tech or stay a mildly convenient peripheral. For one, you could switch the motivational focus from gaining achievements to maintaining them, as many people are more incentivized by loss. You could also shift focus away from gamification (features like point scoring, competition, etc.) to community support—which seems to be taking off. Over the past few years, Fitbit in particular has beefed up its social community with feeds, sub groups, and video-based training. Other solutions could potentially include insurers and employers giving financial incentives to employees to use wearables. But it mostly boils down to a vaguely defined human element.

The fact is, some people will never need a wearable to motivate themselves. Others will do much better with a wearable plus a personal trainer. And others still will find that they thrive with the quantification and competition they can get from wearables alone. I will likely vacillate between weeks of hyper intensity, weeks when I kinda just do my thing, and weeks when I don't wear one at all.

Doctors may see an inherent value in tracking certain health conditions. Or they may not. In the future, you might find it helpful to track your blood pressure with a wearable. You might also decide you'd rather jump out a window than constantly quantify yourself in that way. There are hundreds of thousands of millions of people, and no one solution will fit everyone.

In the end, having enough different types of solutions, so that you can figure out what works best for you, may be the best answer. And wearables will likely range as widely as humans themselves.

“Even if you're not a self-quantifying nut, the benefits of knowing your own body can't be discounted.”

Two-Factor Authentication: Who Has It and How to Set It Up

BY ERIC GRIFFITH

In 2014, the Heartbleed exploit left everyone's login information potentially up for grabs, thanks to one itty-bitty piece of code. In the past few years, our security nightmares have only gotten worse. What can you do to stay safe? Well, you should definitely change your passwords—on a regular basis. Even so, whether compromised by sheer brute force or simple phishing, passwords alone aren't enough protection.

That's why many internet services have embraced two-factor authentication for their users. It's sometimes called 2FA and can be used interchangeably with the terms "two-step" and "verification," depending on the marketing. But what is it, exactly?

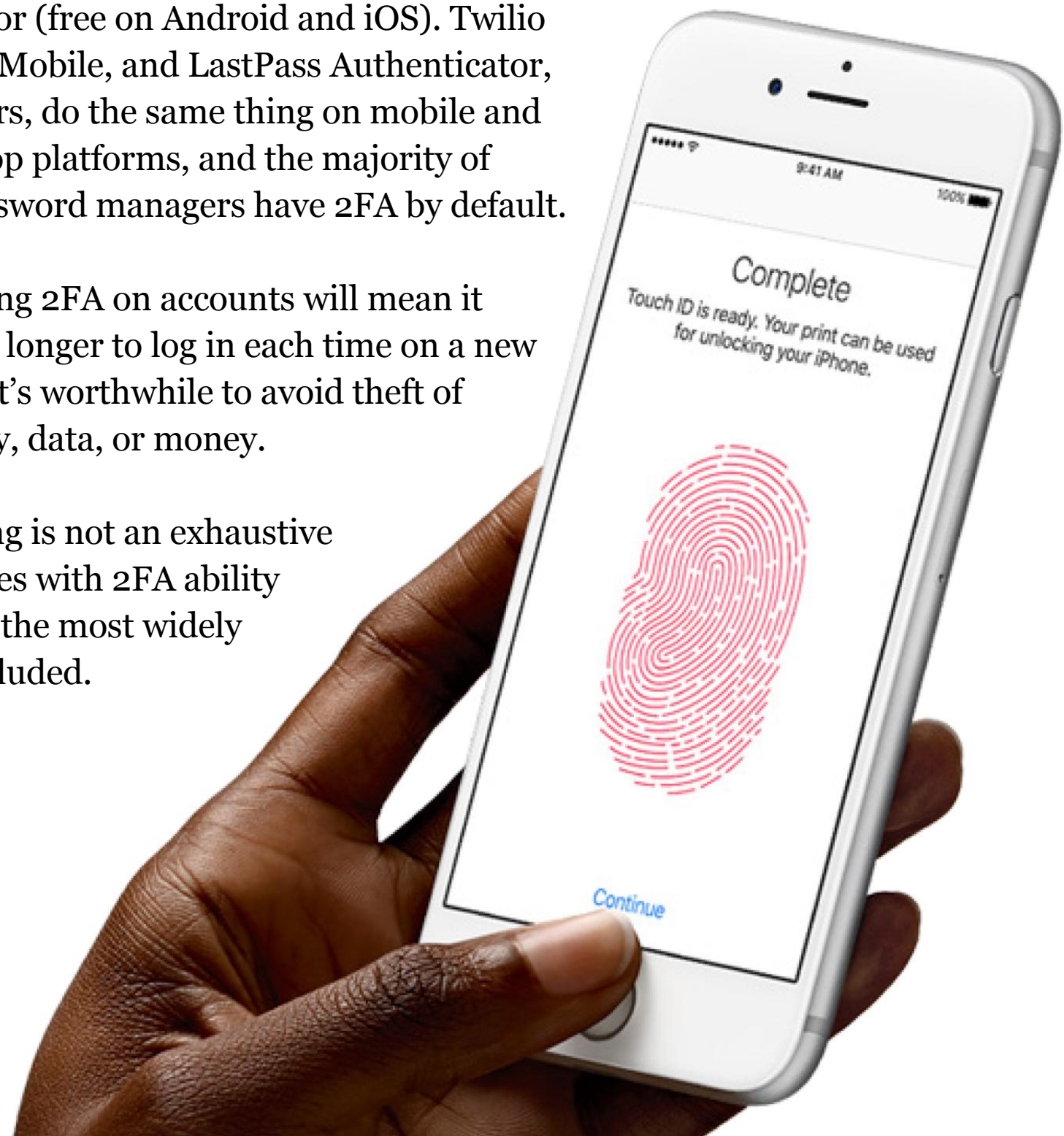
As PCMag's lead security analyst Neil J. Rubenking puts it: "There are three generally recognized factors for authentication: something you know (such as a password), something you have (such as a hardware token or cell phone), and something you are (such as your fingerprint). 'Two-factor' means the system is using two of these options."

Biometric scanners for fingerprints and retinas or faces are on the upswing thanks to innovations such as the iPhone X's Face ID and Windows Hello, but they're still far from ubiquitous. In most cases, including 2FA for your Google account and other popular services, the extra authentication is simply a numeric code—a few digits sent to your phone that can be used only once.

Many services support a specialized app on the phone called an "authenticator" that will do that same job. The app, preset by you to work with the service, has a constantly rotating set of codes you can use whenever needed—and it doesn't even require a connection. The arguable leader in this area is Google Authenticator (free on Android and iOS). Twilio Authy, Duo Mobile, and LastPass Authenticator, among others, do the same thing on mobile and some desktop platforms, and the majority of popular password managers have 2FA by default.

Implementing 2FA on accounts will mean it takes a little longer to log in each time on a new device, but it's worthwhile to avoid theft of your identity, data, or money.

The following is not an exhaustive list of services with 2FA ability but some of the most widely used are included.



GOOGLE 2-STEP VERIFICATION

With access to your credit card (for shopping on Google Play), important messages and documents, and even your videos on YouTube—essentially your whole life—a Google account has to be well protected. Google 2-Step Verification is about identifying you via phone. When you enter a password to access your Google account for almost any service and 2-Step Verification is on, multiple options can get you to that second step. First among them now is the Google Prompt: You simply add your smartphone to your account, make sure the Google search app is on the phone, and at login, you go to the phone and acknowledge with a tap that you are the one signing in. Easy.

If that doesn't work, you'll need to enter an extra code, which is sent to your phone via SMS text, a voice call, or by using an authenticator app. On your personal account, you can register your computer so you don't have to enter a code during every sign-in. If you have a G Suite account for business, you can choose to receive a code every 30 days only.

Google Authenticator—actually, any authenticator app—can generate the verification code for you, even if your smartphone is not connected to the internet. You must sign up for 2-Step Verification before you can use it. The app will scan a QR code on the desktop screen to give you access, then generate a time-based or counter-based code for you to type in. It replaces getting the code via text or voice calls or email. Authenticator apps also work with other services, like LastPass, WordPress, Facebook, Evernote, Microsoft, IFTTT, Dropbox, Amazon, and Slack.

Once you've set up Google 2-Step Verification, access it again by visiting your Google account security settings. There you can select the phone numbers that can receive codes, switch to using an authenticator app, and access your 10 unused codes that can be printed to take with you for emergencies (such as if your phone dies and you can't get to the authenticator app.)

FACEBOOK LOGIN APPROVALS

Access Login Approvals on the desktop by going to Settings > Security. Click Edit next to Login Approvals and Enable on the top right. Facebook defaults to having you authenticate via a Code Generator. You can do so via Facebook's built-in Code Generator or a third-party app.

To use the Facebook app, log in to a new Facebook session somewhere—say, a friend's PC. When prompted for a code, navigate to the Code Generator in the Facebook app () > Code Generator), which displays a six-digit number you type into the browser on the new PC; that number changes every 30 seconds.

If you want to keep all your codes in one place, use a third-party code-generating mobile app (such as Google Authenticator or Authy). Set it up on Facebook.com via Settings > Security > Login Approvals > Edit > Code Generator > Set up another way to get security codes. That will produce a pop-up with a QR code. Open your Authenticator app on your phone, aim it as the QR code on your PC's screen, and you're all set. When you sign in to Facebook from an unknown browser and it prompts you for a code, open the Authenticator app and type in the six-digit code in the Facebook section.

If you'd rather get a text message with a code than use a Code Generator, look for the "need another way to authenticate?" prompt when you sign in. If you have a phone number linked to your Facebook account, clicking that will give you the option to "Text me a login code."

These options require you to have access to your phone, of course. But when you activate Login Approvals, you can get a list of 10 recovery codes that you can download and use at any time, even if you don't have your phone. Get them on Facebook.com > Settings > Security > Login Approvals > Edit > Recovery Codes > Get Codes and save them somewhere safe.

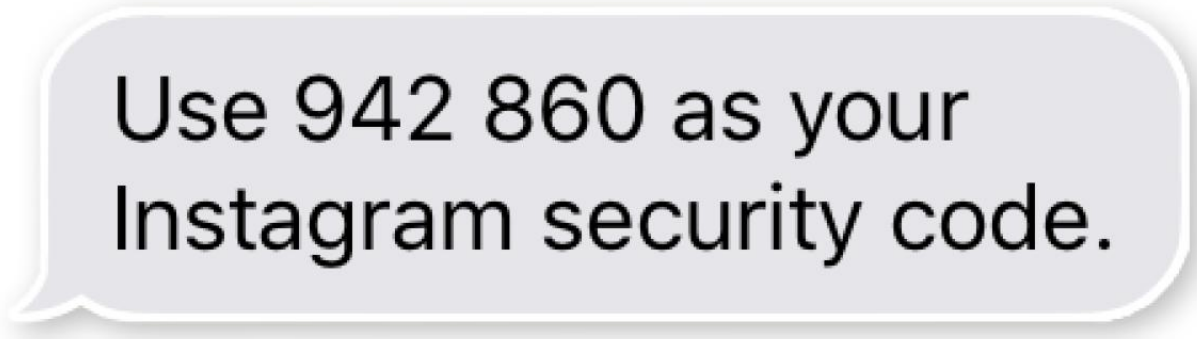
Facebook has even added Security Keys (using USB or NFC capable devices as a key). Not that many people have them, but if you have one, consider using it. Just don't forget to take it with you.

App Passwords is another Facebook security feature. Use them to skip the Login Approvals process altogether by generating a one-time password to access your Facebook account via any third-party app or service. If you log out of that app or service and need to go back in, you'll have to generate a new, unique app password. This is necessary for older devices and versions of apps like Xbox 360, Skype, and Spotify, which can't use Login Approvals, but still benefit from Facebook access.

Instagram, owned by Facebook, started a slow rollout of two-factor authentication to test users in 2016.

INSTAGRAM TWO-FACTOR AUTHENTICATION

Instagram, owned by Facebook, started a slow rollout of two-factor authentication to test users in 2016. To turn it on, look under Settings for Two-Factor Authentication. Turn on "Require Security Code" and add your phone number. Include the country code, because Instagram is everywhere. You'll get a confirmation code via SMS text message. Enter it and 2FA is on.



The app then brings up a list of five backup codes you can use in the future to turn off 2FA. It even offers to take a screenshot of them to add to your camera roll; you can always re-access them in the app as well. In the future, you'll just get another 2FA code if you have to sign in again using a different device.

WHATSAPP

With well over a billion users and worries aplenty these days about people hacking phones, WhatsApp introduced end-to-end encryption as well as two-step authentication to keep out snoops, be they at home or sitting right there at the NSA, CIA, and FBI (Hi, Agent Mulder!).

Setup is easy: Go into Settings > Account > Two-step verification. Click Enable and things get a little different here: WhatsApp asks you for a six-digit PIN to use to register your phone number with WhatsApp. You'll also provide an email in case you ever need to do a reset—aka, turn off the verification. If you later sign out or log in with a different device, WhatsApp will text you a code, then you have to re-enter the PIN as well.

TWITTER LOGIN VERIFICATION

To activate Login Verification on Twitter.com on the desktop, click your profile photo on the top right > Settings and privacy. Under Security, check the box next to Login verification. In the mobile app, go to the Me menu (your profile pic at the upper left), Settings and Privacy > Account > Security > Login verification. Toggle it on (or off).

In the initial setup process, Twitter sends a code via text to your mobile phone. If you go the SMS route, you only get to use one phone for one account and obviously have to associate the number with your Twitter account. (You need the number associated either way—it's used to recover an account you can't access.)

The best option is to select "Setup a code generator app" and scan the QR code that comes up. (If you already have basic phone-based login verification turned on, you can set up the Authenticator app on the desktop by going to Security and clicking "Review your login verification methods," then going to Reverify to set up a mobile security app by scanning a QR code.) The app could be an authenticator like Authy, but you can use the Twitter mobile apps themselves to generate the authentication codes for you.

Twitter can also generate login codes for the times you can't get a 2FA code from a text or authenticator app. Go to Settings > Account > Security > Login code generator. Like with any code generator, it updates every 30 seconds.

Both of those menus also offer the option for a Backup code—take a screenshot and save it in a safe place.

App passwords also allow for one-time use of Twitter in third-party apps. Get one on Twitter.com via the Password tab in Settings; just click Generate. On mobile, go to Settings > Account > Security > Temporary password. The temp is usually a 12-character combo of letters and numbers; it's good for about an hour.

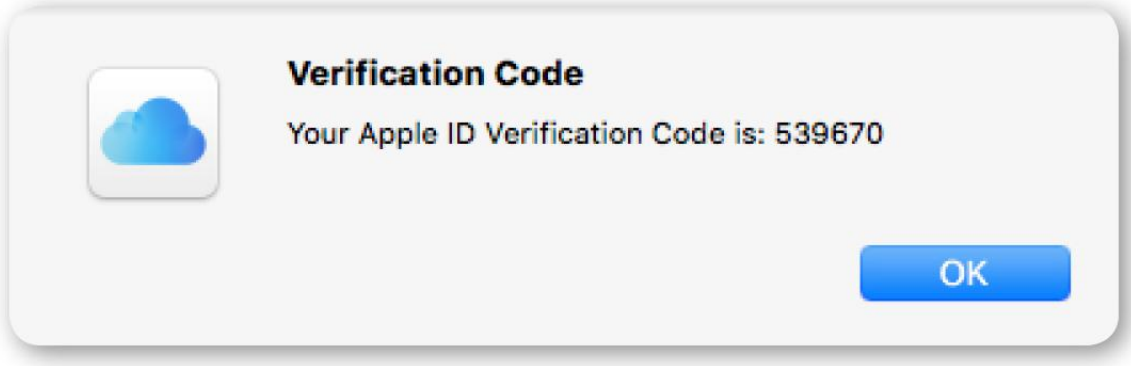
A good rule of thumb: Occasionally view the full list of applications that have access to your Twitter or that use your Twitter credentials and nix any you no longer use or recognize.

Twitter can also generate login codes for the times you can't get a 2FA code from a text or authenticator app.

APPLE TWO-FACTOR AUTHENTICATION

Your Apple ID is a big part of your life if you're an iOS or Mac user. It's important for not just access, but also for storage via iCloud, purchases at iTunes, iBooks, and the App Store, and membership at Apple Music.

To activate two-factor Authentication, go to the My Apple ID page and sign in. Look for Security > Two-Factor Authentication and click "Get Started..."



You are then furnished with steps on how to set up 2FA for Apple using either an iOS device or via macOS. You can't do it via a browser on another operating system anymore. On iOS you go to Settings > iCloud, sign in, tap the arrow next to your Apple ID > Password & Security > Turn on Two-Factor Authentication. On macOS go to > System Preferences > iCloud, sign in, click Account Details > Security > Turn on Two-Factor Authentication.

You'll have to answer two of your three preset security questions and re-confirm your credit card on the account to get into the setup. Then you have to enter a valid phone number to get a text or phone call (even if it's the number already on the phone you're using for setup). If it is the same phone, the six-digit code will be entered automatically when it arrives, or just type it in.

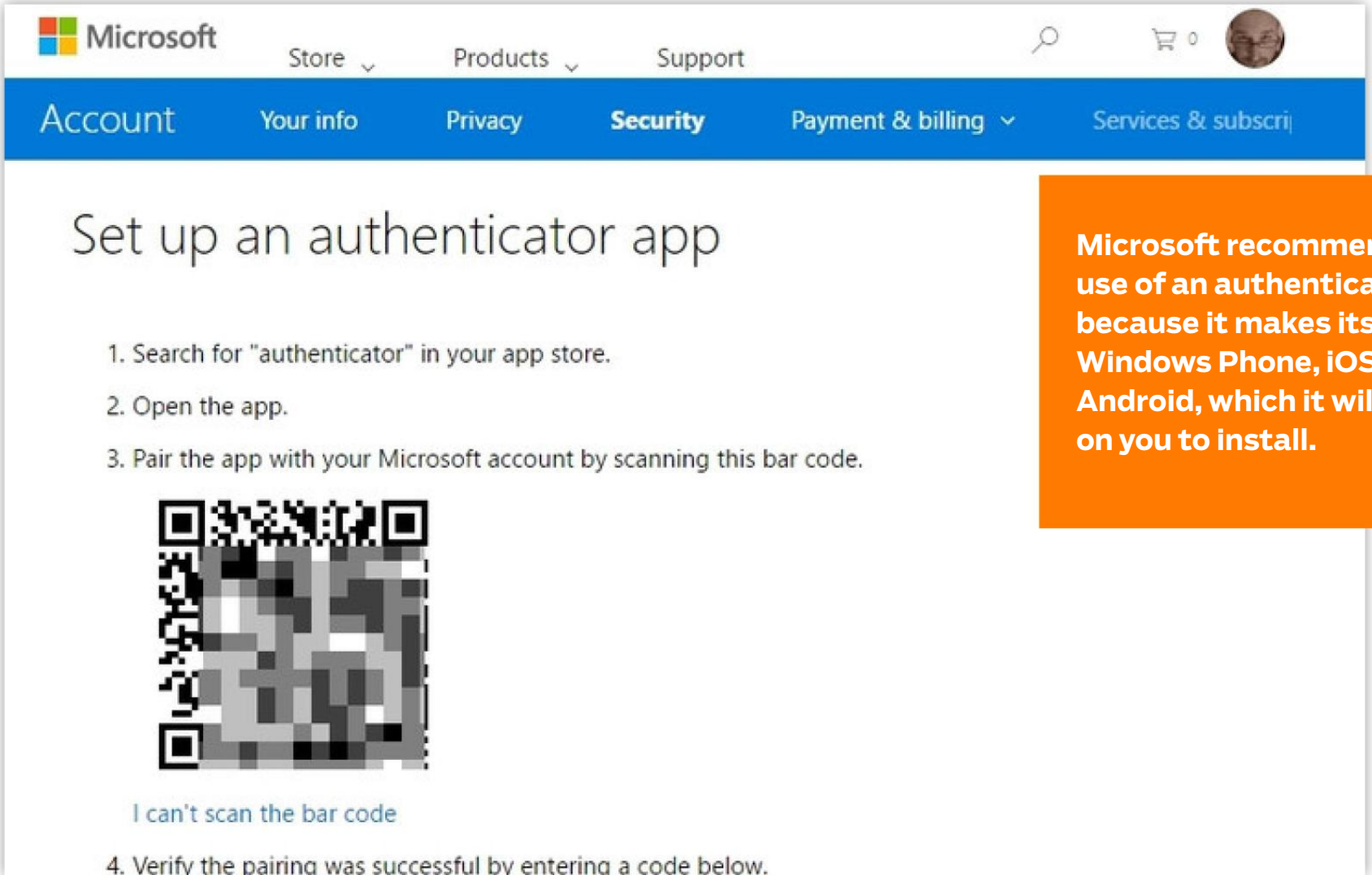
To get a code when needed, go back to iCloud settings, tap your username at top (you'll likely need to enter your full Apple ID password again) > Password & Security > Get Verification Code. This means sometimes you enter a circular-logic world where you need to get a code on the very device where the code has to be entered.

Apple also supports app-specific passwords.

You can turn off Apple 2FA in iCloud settings, but then you have to go back to security questions ("Who was the best man at your wedding?" and the like) to verify your ID, and no one wants that.

MICROSOFT TWO-STEP VERIFICATION

Microsoft has done a much better job in the last few years of tying together all its services under one umbrella account. I use mine for Outlook.com, OneDrive, Xbox Live, Skype, an Office 365 subscription, and more. Naturally, it should get some extra protection.



Microsoft recommends the use of an authenticator app because it makes its own for Windows Phone, iOS, and Android, which it will push on you to install.

You sign into your Microsoft account at account.microsoft.com/profile. In the top navigation, click Security; on the next page, click the more security options link. Scroll down to Two-step Verification to turn it on.

Microsoft will first suggest you get an app password to set up Outlook.com to sync with email on mobile devices, as well as other services that may need app passwords, which you can go in later to generate for any given app.

You can then enter the “Set up an identity verification app” section. Microsoft recommends the use of an authenticator app because it makes its own for Windows Phone, iOS, and Android, which it will push on you to install. It also works with other standard authenticator apps, like Google Authenticator and Authy—but to use them, you must pick “other” during the setup. Scan the QR code displayed.

You can skip the authenticator. If you do, Microsoft logins will still try to get you to use an app, but provide a link to other methods for getting a 7-digit verification code: text or email. Even if you choose text, it has to go to a phone you’ve pre-registered, and even then, Microsoft will make you re-enter the last four digits of the phone number as an extra bit of confirmation.

As you continue the setup, Microsoft provides a recovery code for you to write down and keep safe, a 25-digit whopper (like the kind it uses on everything from software registrations to Xbox giveaways). Microsoft also supports Trusted Devices, which is hardware that doesn’t require you to enter any codes—you’ll see a checkbox to mark a device (like a Windows 10 PC) as trusted when you log into it. Go back to security settings to revoke trusted devices all at once if you lose one. Microsoft automatically removes any trusted device you haven’t logged into in two months; just trust it again on the next login.

How to Use Apple Pay Cash

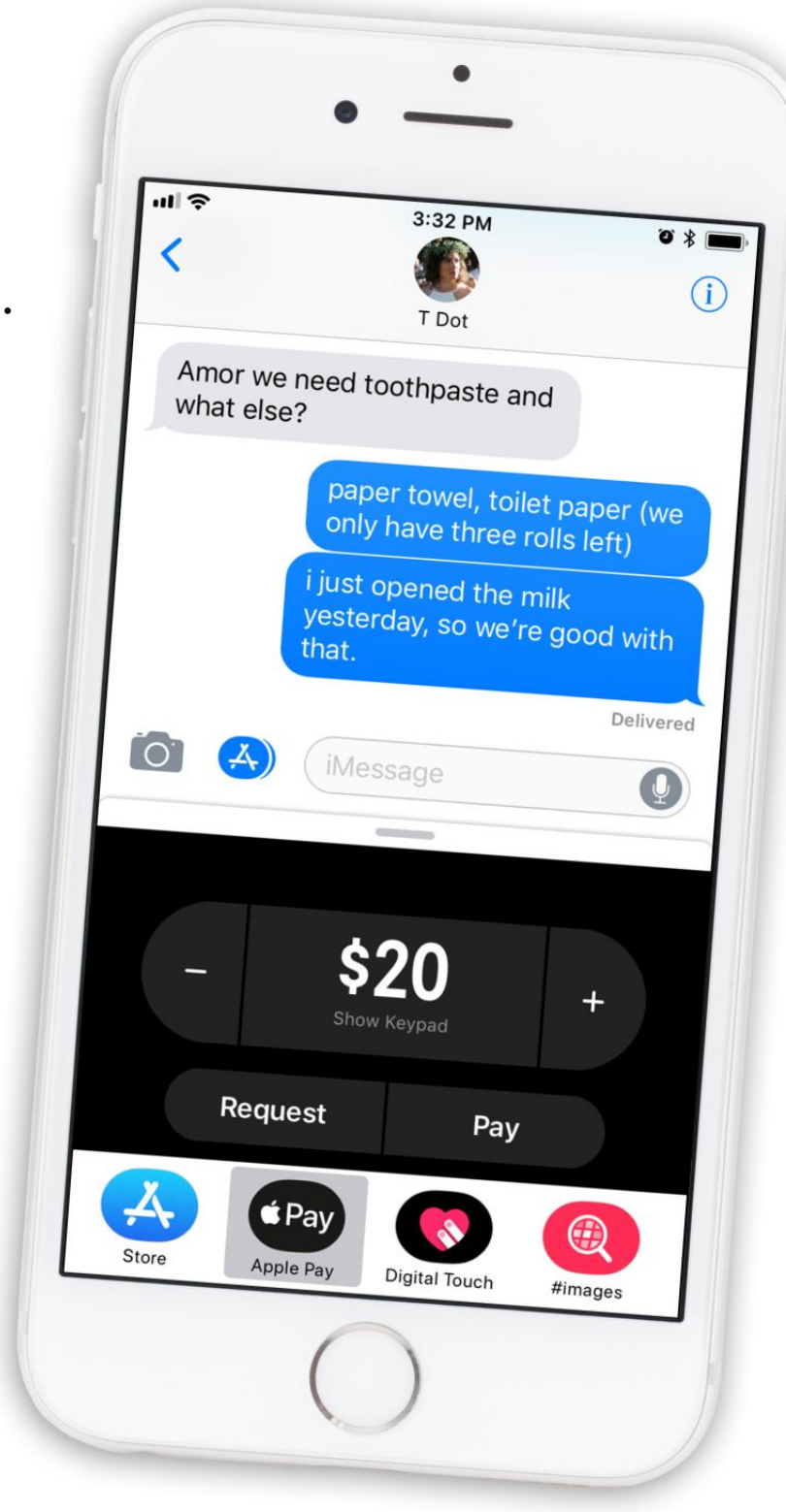
BY LANCE WHITNEY

Want to be able to send someone money using your smartphone? Those of you who use Apple Pay on your iPhone, iPad, or Apple Watch should check out Apple Pay Cash. Apple Pay lets you use your phone to pay for things at physical stores including Sephora and Panera Bread, as well as within certain apps. And Apple Pay Cash lets you send money to someone else as easily as you might send them a text message.

Apple Pay Cash, which rolled out with iOS 11.2 and watchOS 4.2, can be linked to a credit or debit card; a debit card is the better option, since a credit card transaction socks you with a 3 percent fee. You can add more than one card to Apple Pay, so you can set up a credit card for regular transactions and a debit card for Apple Pay Cash.

On the other end, your recipient must also use an iOS device (sorry, Android users). They'll receive an Apple Pay Cash virtual cash card, which can be used to purchase items via Apple Pay or transferred to a bank account.

To send and receive money using Apple Pay Cash, you must be at least 18 years old and live in the US. Your iPhone or iPad has to be compatible with Apple Pay, and you need to enable two-factor authentication (2FA) for your Apple account.



1. OPEN AN iMESSAGE

You can send money through Apple Pay Cash using iMessage or by talking to Siri. To send via Messages, open the app and start a new conversation or open an existing one to the person who will receive the cash. You can send someone money without typing an actual text. But you may want to remind the person why you're sending money; if so, type a message in the text field. Then tap on the app icon on the left and tap the Apple Pay icon.

2. CHOOSE AMOUNT

Tap on the plus or minus key until you see the amount you wish to send. To enter a specific amount instead, tap on the Show Keypad button and then type the amount. At the keypad, you can tap on the Pay button to initiate the payment. Or you can tap on the down arrow to close the keypad screen and return to your message and then tap on Pay.

3. AGREE TO TERMS AND CONDITIONS

At the next screen, tap on Continue. Tap on Agree to agree to the terms and conditions. The next screen tells you that it's setting up Apple Pay Cash.

4. CONFIRM PAYMENT

You're prompted to add a debit card if you don't have one set up to avoid incurring the bank fees charged with a credit card. Add your debit card if necessary. Then return to your text message. Tap Pay. Tap on the Send button in the message to send the payment. Use Face ID, Touch ID, or a passcode to confirm the payment.

5. TROUBLESHOOTING

What if the Apple Pay Cash payment won't go through? In my case, the feature didn't initially work on my iPhone X. Here's what I did to fix it, with help from Apple tech support. First, I turned off Apple Pay Cash and then turned it on to set it up again. To do this, go to Settings > Wallet & Apple Pay. Turn off the option for Apple Pay Cash. Turn it back on. You're asked to type your Apple ID password. Apple Pay Cash then takes you through the setup process once more.

6. VERIFY YOUR IDENTITY

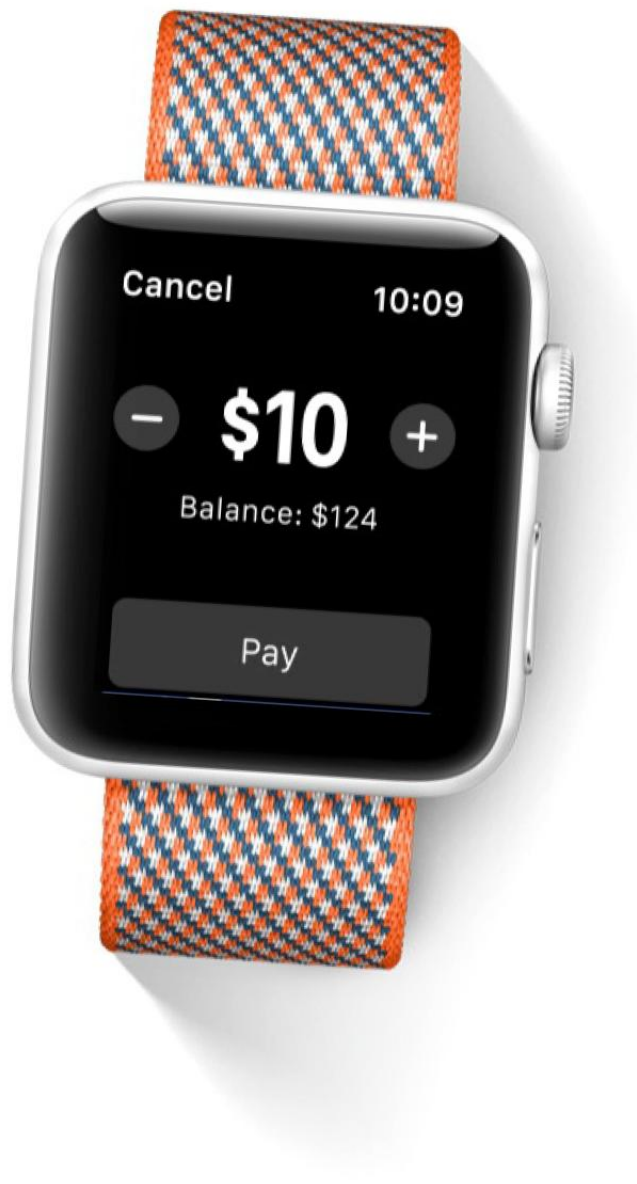
Still not working? Then you may need to verify your identity. To do this, go back to Settings > Wallet & Apple Pay. Under Cards, tap on the entry for Apple Pay Cash. Tap on the link to Verify Identity. At the first screen, type your first and last name. At the next screen, type your address. Next, type the last four digits of your Social Security number and enter your date of birth. After you've finished the verification process, try Apple Pay Cash again.

7. START SENDING MONEY VIA iMESSAGE

After the initial setup, the process for sending someone money is much quicker. Open iMessage and start or resume a conversation with your recipient. Then follow the steps to choose the amount and send the money.

8. GET SIRI INVOLVED

To use Siri to send someone money via Apple Pay Cash, say something along the lines of: “Hey Siri, Apple Pay 25 dollars to Stephen for dinner” or “Hey Siri, send 25 dollars to Stephen.” By default, your Apple Pay Cash payment takes the necessary funds from your debit card. But you can also fill your Apple Pay Cash coffers with more cash through your linked debit card. Tap on Settings > Wallet & Apple Pay. Under Cards, tap on Apple Pay Cash. At the Apple Pay Cash screen, tap on the link to Add Money. At the next screen, enter the amount you wish to deposit. The minimum is $10. Tap Add. Authenticate the transfer with Face ID, Touch ID, or your passcode. You’ll then see the amount listed as your Apple Pay Cash balance.



9. APPLE WATCH

To send money via Apple Pay Cash on an Apple Watch, set up a debit card for Apple Pay for your watch. When you set up a debit card for Apple Pay on your iPhone, you should be asked if you want to use the same card on your paired watch. Open iMessage and start a new conversation or resume an existing one. Swipe down and tap on the icon for Apple Pay. You can choose an amount by tapping on the plus or minus button, turning the Digital Crown, or tapping on the dollar amount and then turning the Digital Crown to select a specific number. Tap on the Pay button. Double-click the side button to pay. Your payment then goes through.

10. RECEIVE A PAYMENT

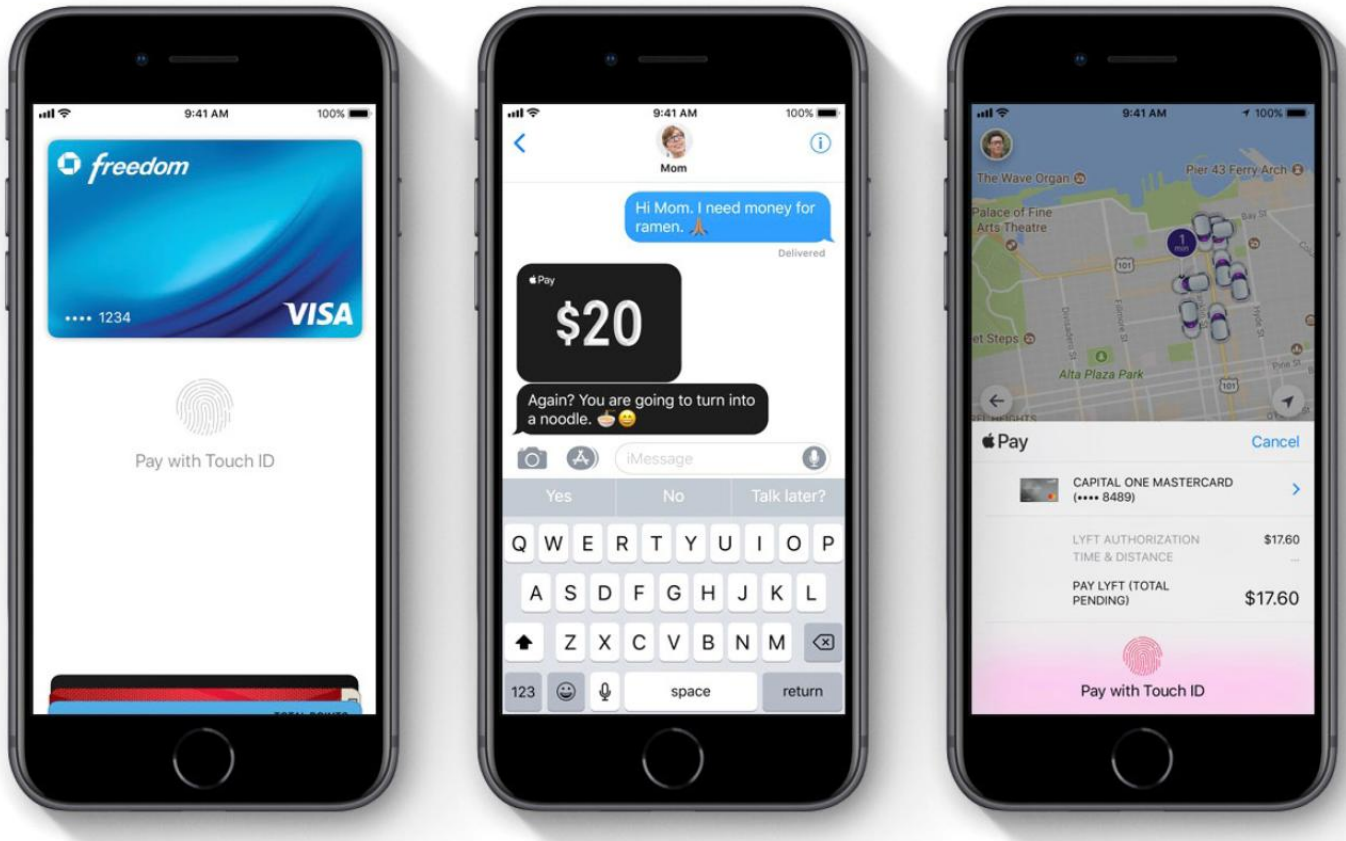
You can also request money from someone else. Open a conversation in iMessage. Tap on the App button and Apple Pay Cash if it’s not already selected. Choose an amount and tap on the Request button. Add a comment to the message and tap on the button to send it. On the other end, your recipient receives the request as a text and just taps on the Pay button to pay it.

11. MANUALLY ACCEPT PAYMENTS

By default, payments via Apple Pay Cash are automatically accepted. But you can change this to Manual mode, which means you must actively accept the payment within seven days. Return to the Apple Pay Cash card screen under Settings > Wallet & Apple Pay. Under the section for Accepting Payments, change the option to “Manually Accept Payments.” At this same screen, you can also tap on the Transactions tab to see all your Apple Pay Cash transactions. At the bottom of the Transactions screen, tap on the link to Request Statement to receive an email of your transactions.

12. ADD YOUR BANK ACCOUNT

What can you do with money you receive via Apple Pay Cash? You can tap into that balance to pay for something using Apple Pay or you can transfer funds to your bank account. To cash out, you’ll need to add your bank account and routing number. Return to the Apple Pay Cash card screen under Settings > Wallet & Apple Pay. Under the section for Balance, tap on the link to Transfer to Bank. Tap on the button to Add Bank Account. Enter your bank’s routing number and your account number. Enter the amount of money you want to transfer and then tap on Transfer. Confirm the transaction via Face ID, Touch ID, or your PIN. The money typically takes one to three business days to end up in your account.



How to Build a PC in 2018: Choosing the Right Components

BY JOEL HRUSKA

The actual assembly process isn't usually all that difficult, but choosing the right components for a build-it-yourself PC can be tricky. We're here to help.

CASE

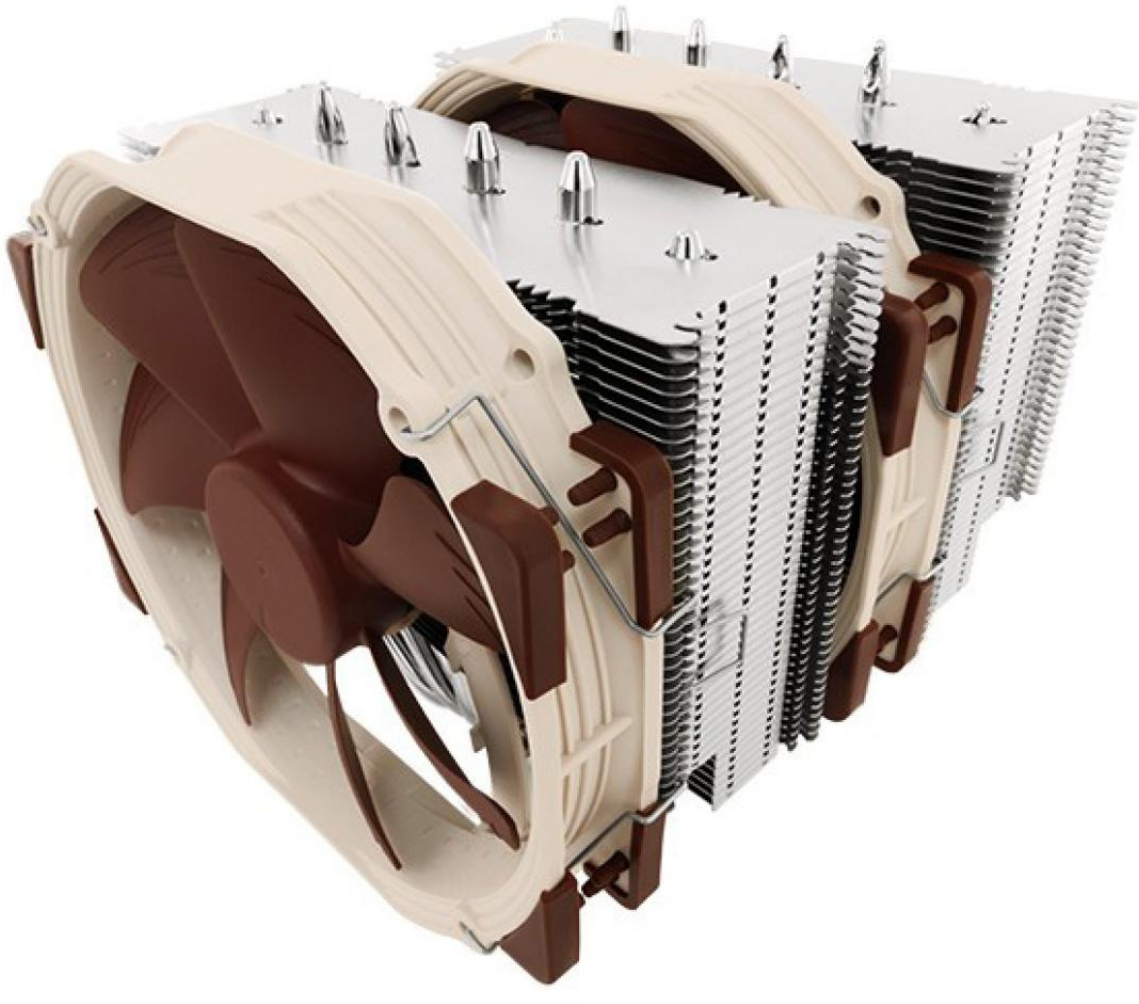
Although components such as the CPU and GPU will determine what your machine can do in an absolute sense, the chassis you pick is still important. The PC case determines which kinds of CPUs and GPUs you can install, what your peripheral and storage options are, and which cooling equipment can be installed. You may not plan to open it often or to change the installed equipment, but every interaction you have with your system will happen through and around the case it uses.

Cases tend to be marketed as one of several types of tower—full tower, mid tower, and mini tower are the three basic categories, along with a few for literal "desktop" machines (HTPC). There's some overlap between case and motherboard sizes, so I'll address that question more fully later on. Small cases are typically harder to work in, because they give you less room to maneuver when installing or removing components, and also because you may have to install hardware in a specific order. Some towers, for example, allow you to access the rear of the motherboard to remove a bolted-on heatsink without having to pull the entire motherboard to do it. An HTPC case isn't going to offer that kind of benefit.

The other advantage of larger cases, to be honest, is that they let you be lazier. Need to install a new SSD or HDD, and don't feel like taking the old one out? No problem. Leave it right where it is. There's usually not much difference in connectivity—small PCs can rival large ones when it comes to USB ports and other peripheral options, if they're designed to do it.

COOLING

PC cooling options range from the heatsinks AMD and Intel ship with their own boxed processors to various esoteric multi-stage freon units and fanless oil immersion rigs. Most enthusiasts opt for more prosaic air cooling methods.



The Noctua DH15 is a high-end cooler—most are not this large and don't use dual fans.

The typical CPU coolers from AMD and Nvidia will absolutely keep your CPU within normal operating temperatures and running fine even under load. You don't need to spend money on an aftermarket cooler at all if you don't want to. If you do buy an aftermarket cooler, make sure to check its intended motherboard orientation, maximum cooler height (when installing it into a smaller chassis), and whether it makes installing RAM difficult. This last is a common issue; when installed, many aftermarket CPU coolers partially overhang RAM sockets. Since most RAM these days has heatsinks of its own, this can make installing or swapping RAM challenging.

If I had to pick one CPU cooler brand to recommend, it'd be Noctua. Its coolers aren't particularly inexpensive, but they come with extensive, full-color instructions; they include installation hardware such as screwdrivers; the build quality of Noctua fans and heatsinks is excellent; and the company offers an excellent upgrade policy.

In many cases, Noctua offers upgrade kits that will allow you to keep using an older cooler on a newer motherboard. Given that CPUs have topped out at roughly 140W (with a handful of exceptions) for a decade, this is a great way to keep using a valuable component that can cool a newer chip just as well as an old one.

A Noctua NH-U14S, installed. Note the way the cooler overhangs the RAM slots.

Note that CPU coolers are typically rated in terms of their TDP (thermal design power). This is the amount of heat the cooler is designed to dissipate over a given period of time and should be matched to the listed TDP of the CPU at minimum. It's fine to use a cooler that can handle a 150W TDP on a 50W chip, but don't try using a 50W cooler on a 150W CPU. It won't fry—we're a bit past that point now—but the system may destabilize and will run slowly.

MOTHERBOARD

The motherboard you pick shapes what your system is capable of and how much expandability you can expect in the future. The three basic motherboard types in the consumer market, in order of size, are Mini-ITX, Micro-ATX (mATX), and ATX.

ATX motherboards are full-size standard consumer products, typically with seven expansion slots. mATX boards are shorter and offer fewer slots, and ITX boards have the fewest expansion and memory slots. If you're not sure which you want, consider this: Most users won't notice the difference between an ATX versus an mATX board as far as useful onboard features or capabilities, while an ITX board does require various meaningful tradeoffs even on low-level features.

A decent rule of thumb: When you know you need a Mini-ITX board for a specific project, that's one thing, but you'll probably want something larger for any general use system.

The motherboard shapes what your system is capable of and how much expandability you can expect.

As you shop for a case, you'll see them labeled "ATX Full Tower," "ATX Mid-Tower," and so on. Any chassis labeled ATX should be capable of handling a full-size ATX motherboard. Each case should specifically state which motherboard form factors it supports, including workstation motherboard standards such as EATX that we're not discussing here.

The difference between an ATX Full Tower and an ATX mini tower, when both support a full-size ATX motherboard, will be the height and clearance within the case itself. Your GPU and cooler options may be constrained if you opt for a small tower, even if the motherboard itself always fits into the available space.

“Your GPU and cooler options may be constrained if you opt for a small tower, even if the mother-board fits.”

CPU

The CPU you pick determines your motherboard. The motherboard you pick determines your CPU (and your RAM type). Confused? Keep reading.

CPUs fit into sockets on motherboards, which means the motherboard has to have the appropriate number of pins (or holes, in AMD's case). This is commonly referred to as a socket standard. Intel's current socket standard is LGA1151, and AMD's is Socket AM4.

The combination of the CPU and motherboard you choose determines your RAM type. We have to say "combination," because in some cases, CPUs have supported multiple types of DRAM—so the standard you used was a question of which your motherboard supported. Generally speaking, the motherboard box will tell you which is which, and given that DDR3 is on its way out, DDR4 should be the only solution you really have to worry about as far as DRAM is concerned. Whether you'll be able to afford DRAM is another question.

Past the question of socket compatibility, your CPU choice has knock-on effects on the rest of the system build. Higher-end CPUs typically draw more power, and you may want to use a better cooler with top-end models. Always make sure to match your CPU's listed TDP with the TDP of the cooler you're using (CPUs shipped from AMD and Intel will come with an appropriately rated CPU cooler when you buy retail packaged parts).

GPU

GPU prices are currently so inflated that my advice is not to buy a GPU at all and make do with whatever you've already got, buy used, or otherwise limp along until the cryptocurrency market calms the hell down.

GPU prices are so inflated that my advice is not to buy a GPU at all and make do with whatever you've already got.

Apart from that minor problem, the two big GPU issues to be aware of are the physical size of the card and its overall power consumption. GPUs are typically defined in terms of the number of slots they take up inside the chassis and the physical length of the card. Dual-slot cards are now the norm across most of the market, since this design allows for larger, quieter coolers, but it also means you need a certain minimum footprint within your case. When picking out a motherboard, make sure to account for this.

The Radeon R9 295X2, currently the longest GPU I'm aware of, at over 12 inches.

The other physical constraint to be aware of when buying a GPU is length—and this plays into what kind of chassis you buy. Any ATX chassis should hold an ATX motherboard, but ATX motherboards are only 9.6 inches wide. Because some smaller chassis allow the drive bays to partially overlap the motherboard tray, you can wind up with a case that has less than 9.6 inches of room for a GPU, even though the case itself claims compliance with the ATX standard.

POWER SUPPLY

When choosing a power supply unit (PSU), bear several things in mind. First, the PSU has to provide sufficient power for all the components in the system, with some additional room on top as a safety margin. Sites including Newegg have their own power-supply calculators with varying degrees of complexity, depending on how far down this particular rabbit hole you want to jump. Generally speaking, 300W can run a desktop without a GPU, 550W will handle a midrange GPU or below, and a high-end GPU needs at least 600 watts.

> **The PSU has to provide power for all components in the system, with some additional room as a safety margin.**

Second, consider the number of six or eight-pin plugs for powering GPUs. Two eight-pin plugs (or one six-pin/eight-pin combo) can drive a single GPU, while four or more may be needed for multi-GPU configurations.

Again, don't assume that more plugs means the power supply can feed whatever GPU you're considering—the wattage and pinouts both must match the card. The PSU also has to provide enough power over the 12V rails for a high-end GPU, though this shouldn't be an issue for any single GPU system, provided you follow the advice above.

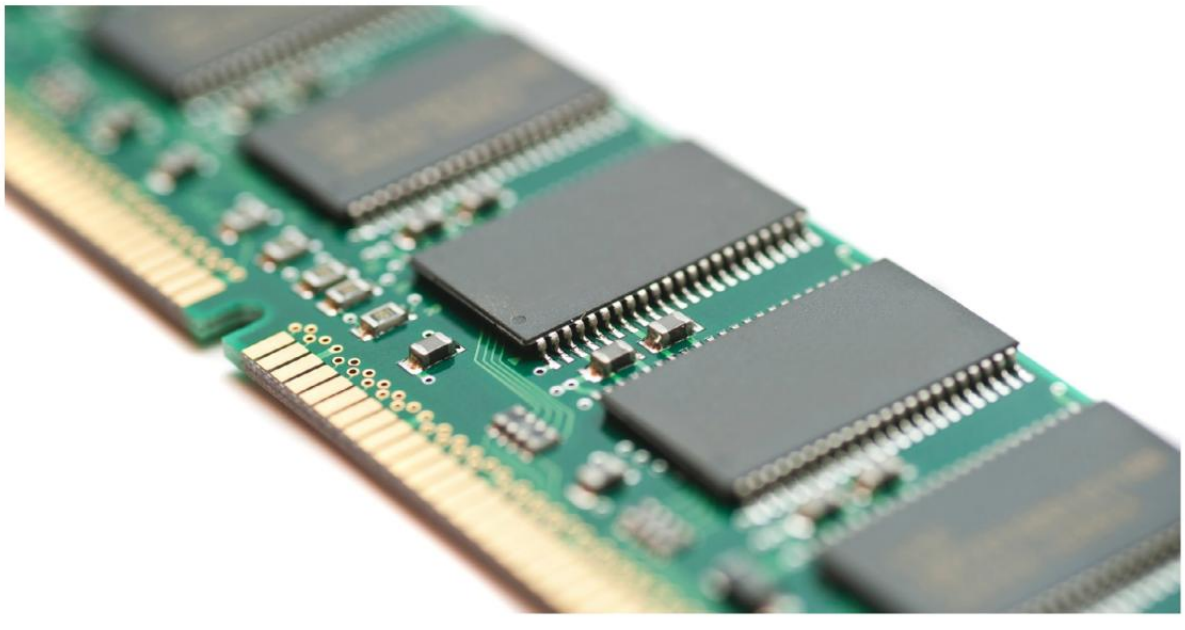
Third, consider whether you want an 80 Plus unit or something that offers a higher level of overall power efficiency. This article should offer some additional context for that decision and some general power consumption advice.

Final point: Do not buy a generic power supply from a no-name vendor. I cannot stress that enough. More often than not, generic PSUs from no-name vendors die at less than half the load they claim to rate. Skimp everywhere and anywhere else, but do not skimp here.

> **Do not buy a generic power supply from a no-name vendor. I cannot stress that enough.**

RAM

RAM prices are also high and may remain that way through the end of 2018. DDR4 is the mainstream memory currently on the market (unless you know you need older DDR3, DDR4 is what you'll likely be buying), but given the current pricing, it's hard to recommend that you splurge.



You'll want to deploy RAM in matched sticks in virtually all cases, but right now our advice is to price for affordable capacity first.

STORAGE

You have two choices: larger and much slower hard drives or faster and smaller SSDs. Generally, an SSD is always the better option, though some users hybridize and use both, with a moderate-sized SSD as a boot drive and preferred application installation platform (256GB or 512GB) and a larger (2TB to 4TB+) data storage partition. Media files and other resources can typically be kept on an old-fashioned spinning disk.

SSDs based on the M.2 standard that interface via PCI Express are also available. These are faster than traditional SSDs, which use SATA (as do HDDs) but require motherboard support. If you are interested in an M.2 PCI Express SSD, make sure your motherboard has the appropriate slot and level of support.

Finally, you can certainly include a Blu-ray drive in your build, provided you pick a case that supports one. Optical media playback isn't as central to PCs as it was 10 years ago, but the option exists. Be advised you'll need a third-party Blu-ray playback solution, and CyberLink PowerDVD is pretty much the go-to.

JOHN C. DVORAK

Is Bitcoin the Biggest Bubble in Human History?

In February, the market finally showed some weakness after a wild post-election stock market run-up, and it's taking Bitcoin with it. At least so far.

A lot of us were amused when Nouriel Roubini of Roubini Macro Associates appeared on Bloomberg Television and said Bitcoin is the "biggest bubble in human history"—worse than Dutch tulips, the dot-com crash, and on and on. (Personally, I prefer the Beanie Babies comparison.)

Three years ago, Bitcoin was under $400, a price I thought was too high even then. As far as I'm concerned, Bitcoin has no intrinsic value and should be worth nothing. So why does anyone think it's worth thousands (and in some cases, millions) of dollars?

It's the theory of false scarcity. There are a limited number of bitcoins in the world, and the usage of blockchain technology has assigned the ownership of each coin to specific wallets owned by individuals. So to take "ownership," I have to use the universal blockchain mechanism, accepted by all as valid, to transfer a coin.

This is an adult form of play money, utilizing a convoluted technology that does not seem to be good for anything besides protecting the conjured coins and making them a scarce "object" with no substance. Hence the "false" part.

@ THErealDVORAK

Plenty of technologists and guys smarter than the average bear are all-in on Bitcoin, because they can see a different reality, like Peter Thiel and Max Keiser. A lot of readers tell me I don't "get" Bitcoin, and I'm blowing it by not getting in on the action. What do they see that I do not, and why do they value this scarcity so much that the sky is the limit insofar as the value is concerned?

Scarcity can often be equated to value. The stock market shows how that can work in a bull market. Also, the art market will reflect it with certain dead artists. But there are plenty of scarce artworks worth nothing. And stocks crash all the time, no matter what the float.

In fact, the way stock certificates are registered and traded seems a lot like Bitcoin. Each share is registered to a person or thing. And they are scarce. Yet they can easily be worth nothing.

Bitcoin fanatics are banking on the value of scarcity. But the point is that scarcity in and of itself has no value, no matter how much it is protected.

The other big theme of Bitcoin is that it can act as a shadow currency to thwart the prying eyes of governments. Things can be bought and sold "off the books." This worked well for drug purchases on Silk Road and for blackmailing schemes and ransomware. It might have continued to work well if the Bitcoin itself was stable. It's not.

Many of the cryptocurrency promoters are paranoid. It's no coincidence that once Ed Snowden revealed that our government is spending more time spying on the public than we

> **The other big theme of Bitcoin is that it can act as a shadow currency to thwart the prying eyes of governments.**

ever could imagine, Bitcoin started to come up in conversations more and more. People believe Bitcoin is the way out of some imagined, repressive capitalist system of horrors.

The whole phenomenon is a never-ending conversation on media outlets like CNBC. Bitcoin is now part of some funds, and is considered a good investment in a diversified portfolio as far as these folks are concerned. You may as well recommend people invest in squid ink.

That said, I personally do not see how this is the mother of all bubbles. That's because the public at large is not yet all-in, like they were with the housing bubble. The mechanism to own Bitcoins is too arcane for most. Previous crashes almost always were designed to fleece the public at large.

In other words, Bitcoin will remain in the conversation until the public buys in. Then it will crash, and finally, nobody will talk about it anymore.

john_dvorak@pcmag.com

MASTHEAD / EDITORIAL

EDITOR-IN-CHIEF, PC MAGAZINE NETWORK Dan Costa
MANAGING EDITOR, DIGITAL EDITIONS Carol Mangis
PRODUCTION DESIGNER José Ruiz

NEWS & FEATURES

EXECUTIVE EDITOR Chloe Albanesius
FEATURES EDITOR Eric Griffith
SENIOR FEATURES WRITER Chandra Steele
SENIOR NEWS EDITOR Matthew Humphries
ASSOCIATE FEATURES EDITOR Rob Marvin
NEWS REPORTERS Michael Kan, Angela Moscaritolo
SOCIAL MEDIA MANAGER Pete Haas

REVIEWS

EXECUTIVE EDITOR Wendy Sheehan Donnell
MANAGING EDITORS Sean Carroll (software, security), Alex Colon (consumer electronics, mobile), Jonathan Rougeot (hardware)
LEAD ANALYSTS Michael Muchmore (software), Neil J. Rubenking (security), Sascha Segan (mobile)
SENIOR ANALYSTS Jim Fisher (digital cameras), Will Greenwald (consumer electronics), Tony Hoffman (printers, projectors, scanners), Jeffrey L. Wilson (software)
ANALYSTS Tom Brant (hardware), Matthew Buzzi (hardware), Max Eddy (software, security), Ajay Kumar (mobile), Victoria Song (consumer electronics)
JUNIOR ANALYST Ben Moore (software)
INVENTORY CONTROL COORDINATOR Alice Newcome-Beill

BUSINESS REVIEWS & SOFTWARE INDEX

EDITOR Oliver Rist
MANAGING EDITOR Suzanne Kattau
SENIOR EDITOR Juan Martinez
ANALYST Rob Watts

PRODUCT & PRODUCTION

DIRECTOR, PRODUCT MANAGEMENT Sarah Shaiq
SENIOR PRODUCT MANAGER Alex Zeng
PRODUCER Gina Latessa
COMMERCE PRODUCER Arielle Rochette

ART & MEDIA

VIDEO MANAGER Jonno Hill
SENIOR VIDEO PRODUCER Weston Almond
STAFF PHOTOGRAPHER Zlata Ivleva
VIDEOGRAPHER Zach Yuzon

CONTRIBUTING EDITORS

Tim Bajarin, John R. Delaney, Jill Duffy, John C. Dvorak, Tim Gideon, Edward Mendelson, Laarni Almendrala Ragaza, Matthew Sarrel

ZIFF DAVIS INC.

CHIEF EXECUTIVE OFFICER (J2 GLOBAL) Vivek Shah

PRESIDENT Steven Horowitz

CHIEF FINANCIAL OFFICER Brian Stewart

CHIEF TECHNOLOGY OFFICER (J2 GLOBAL) Joseph Fortuna

CHIEF STRATEGY OFFICER James Yaffe

GENERAL MANAGER, ZIFF DAVIS TECH/COMMERCE Mike Finnerty

SENIOR VICE PRESIDENT, CONTENT Dan Costa

SENIOR VICE PRESIDENT, SALES AND MARKETING Eric Koepele

SENIOR VICE PRESIDENT AND GENERAL MANAGER, ACCOUNTING Fredrick Rolff

SENIOR VICE PRESIDENT, COMMERCE Jason Steele

SENIOR VICE PRESIDENT, STRATEGY & GROWTH Jason Sinnarajah

GENERAL COUNSEL Stephen Hicks

VICE PRESIDENTS Frank Bilich (media sales), Melissa Hart (marketing), Diane Malanowski (human resources), Archer Rosenblum (technology), Suzanne Sypulski (Operations)

DIRECTOR, FP&A: Megan Juliano

THE INDEPENDENT GUIDE *PC Magazine* is the Independent Guide to Technology. Our mission is to test and review computer- and Internet-related products and services and report fairly and objectively on the results. Our editors do not invest in firms whose products or services we review, nor do we accept travel tickets or other gifts of value from such firms. Except where noted, *PC Magazine* reviews are of products and services that are currently available. Our reviews are written without regard to advertising or business relationships with any vendor.

HOW TO CONTACT EDITORS We welcome comments from readers. Send your comments to pcmag@pcmag.com or to *PC Magazine*, 28 E. 28th St., New York, NY 10016-7940. Please include a daytime telephone number. *PC Magazine*'s general number is 212-503-3500. We cannot look up stories from past issues, recommend products, or diagnose problems with your PC by phone.