IMPROVE WI-FI RANGE ● STREAM MEDIA ● SECURE YOUR NETWORK

BUILD A BETTER HOME NETWORK

Your complete guide to reliable networking

PLUS! ANDROID AND APPLE STREAMING

EASY STEP-BY-STEP WORKSHOPS

TP-LINK®
The Reliable Choice

Faster, Stronger Wireless

For Smoother, Responsive Gaming and Lag Free HD Streaming

AC1750

Cable Connection

Archer C7 Wireless Dual Band Gigabit Router

- Next generation wireless X3 faster than dual band
- Full Gigabit Wired Connections for Ultrafast Data Transfer Speeds
- Simple set up
- Guest network feature to securely share work or home wireless network

Phone Line Connection

TD-W8980
N600 Wireless Dual Band Gigabit
ADSL2+ Modem Router

Cable Connection

TL-WDR3600
N600 Wireless Dual Band
Gigabit Router

TL-WDN3200
N600 Wireless Dual Band USB
Adapter

N600

TL-WA890EA
N600 Dual Band WiFi Entertainment
Adapter with 4 Ports

HEXUS PERFORMANCE

3 Year Warranty

24/7 Technical Support: **0845 147 0017**
Support Email: **support.uk@tp-link.com**

amazon.co.uk

Currys PC World

TP-LINK UK E-mail info@tp-link.com Website www.tp-link.com

Specifications are subject to change without notice. TP-LINK is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders. Copyright © 2013 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved. PN: 8392500477

CREDITS

Editor David Ludlow
Production Editor Steve Haines
Design Billbagnalldesign.com
Photography Danny Bird, Julian Velasquez
Contributors Mike Bedford, Simon Edwards, Kat Orphanides
Digital Production Manager Nicky Baker

MANAGEMENT
MagBook Publisher Dharmesh Mistry
Operations Director Robin Ryan
MD of Advertising Julian Lloyd-Evans
Newstrade Director David Barker
MD of Enterprise Martin Belson
Chief Operating Officer Brett Reynolds
Group Finance Director Ian Leggett
Chief Executive James Tye
Chairman Felix Dennis

MAGBOOK

The MagBook brand is a trademark of Dennis Publishing Ltd. 30 Cleveland St, London W1T 4JD. Company registered in England. All material © Dennis Publishing Ltd, licensed by Felden 2013, and may not be reproduced in whole or part without the consent of the publishers.

Build a Better Home Network
ISBN 1-78106-254-4

LICENSING & SYNDICATION
To license this product please contact Carlotta Serantoni on +44 (0) 20 79076550 or email carlotta_serantoni@dennis.co.uk.
To syndicate content from this product please contact Anj Dosaj Halai on +44(0) 20 7907 6132 or email anj_dosaj-halai@dennis.co.uk.

LIABILITY
While every care was taken during the production of this MagBook, the publishers cannot be held responsible for the accuracy of the information or any consequence arising from it. Dennis Publishing takes no responsibility for the companies advertising in this MagBook.

The paper used within this MagBook is produced from sustainable fibre, manufactured by mills with a valid chain of custody.

Printed by Polestar, Bicester

Welcome!

Because the vast majority of broadband providers give away a free wireless router, most of us now have a home network that we use to share our internet connections. However, it's probably fair to say that many of us don't actually make the most of our home networks.

Beyond simply sharing an internet connection, a properly configured home network can be the perfect way to share files and printers between all your computers. Add a network-attached storage (NAS) device into the mix and you've got always-on storage that everyone can use.

What's more, a NAS can act as a media server for all your digital photos and videos, as well as your entire music collection. That means you can watch or listen to what you want, where you want. Add a smartphone or tablet into the equation for controlling playback and suddenly you have a complete multiroom entertainment system.

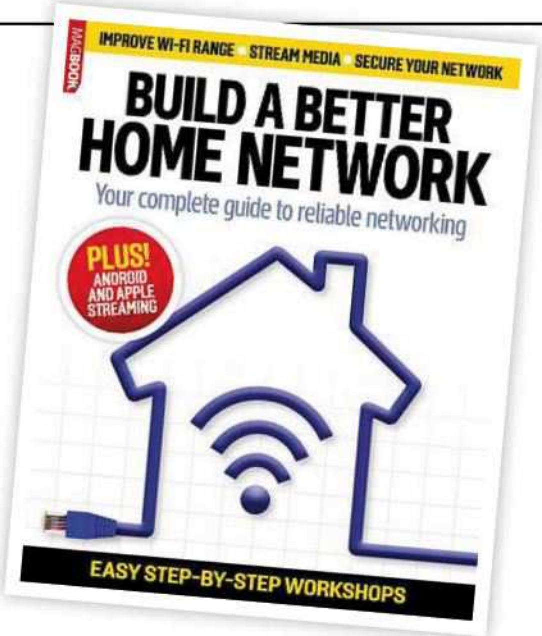
This book tells you more than simply the best way to use your home network, though. We've all suffered from our wireless router dropping the signal in parts of our homes, but wouldn't it be great if you had amazing Wi-Fi coverage everywhere? In this guide we'll show you how to get rock-solid, super-fast wireless all over your home.

Once all your computers are connected to the internet, security becomes a big issue, and you'll need to become more vigilant to protect your data from hackers. We'll show you how to stay safe, deal with threats and even track stolen property online.

Finally, we'll show you how cloud storage can make a huge difference to your digital life, giving you a simple, secure and robust method of backing up all your important files. The main benefit of cloud storage is that it's immune to fire, theft and mechanical failure, making it the perfect way to keep all your precious files safe.

With this guide you'll find that your home network can go from a utilitarian way to share the internet to one of the most important things in your house.

David Ludlow
Editor



MAGBOOK

IMPROVE WI-FI RANGE · STREAM MEDIA · SECURE YOUR NETWORK

BUILD A BETTER HOME NETWORK

Your complete guide to reliable networking

PLUS! ANDROID AND APPLE STREAMING

EASY STEP-BY-STEP WORKSHOPS

Contents

05

STREAMING MEDIA OVER YOUR NETWORK

Learn how to stream photos, videos and music around your home using your PC, TV and a media player, and control everything from your phone or tablet

06

STREAMING MEDIA WITH APPLE KIT

We reveal how AirPlay and Apple TV can integrate seamlessly with the rest of your network to give you the ultimate home entertainment system

07

INTERNET SECURITY

Keep your network and everything on it safe from hackers and viruses with our in-depth guide to internet security

08

THE CLOUD

Without the right backup procedure in place, you could easily lose all our precious digital photos, videos, music and documents forever. Fortunately, the cloud can help you keep everything safe

09

TROUBLESHOOTING

Having problems with your network? Confused by some of the technical jargon? Don't worry: our easy-to-use troubleshooting guide and glossary are here to help you out

1

INTRODUCTION TO NETWORKING

You've got a broadband router and all your devices are connected to the internet, so why take things further? In this chapter we'll show you all the amazing things you can do with a home network, from home entertainment to file sharing, helping you plan what you want to achieve. We'll also take you through some networking basics, so you'll understand how everything's tied together.

CONTENTS

INTRODUCTION TO NETWORKING

1

Top things to do with a home network

We live in a networked world, where not having access to the internet is a massive disadvantage. Even if you're not using the internet, though, having a home network makes a lot of sense, as it makes it easy to share files and printers with other home users.

Add a network-attached storage (NAS) device into the mix, for example, and you'll have some always-on storage that's easy to share between everyone. Then there's the option to stream music and photos over the network, so you can enjoy all your digital media as and when you want.

As you can see, then, having a network isn't just an attractive optional extra: these days it's pretty much a necessity. Here we'll show you some of the best uses of a home network, so you can see just how essential it really is.

Once we've taken you through all the benefits in this chapter, we'll help you get up and running with our in-depth guides throughout the rest of the book.

01 SHARE THE INTERNET

This is probably something you do already, but there's no harm in reiterating just how important this is. With a wireless router you can have every device on your home network connected to the internet. Now that practically every device – from tablets, smartphones and laptops to TVs and Blu-ray players – can connect to the internet, sharing has never been quite to important. To top it all off, we'll show you how to extend your wireless network and get an amazing signal anywhere in your house.

> “We'll show you how to stay protected, how to avoid scams and even how to track and recover stolen laptops and mobile phones.”

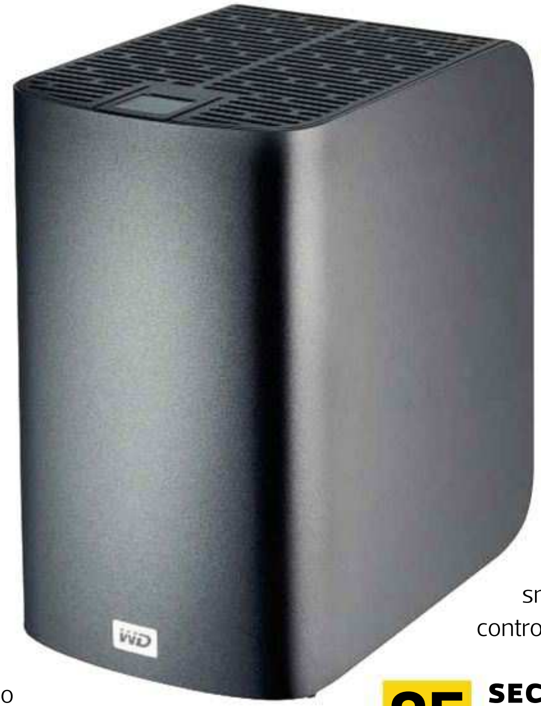
With a home network, a printer attached to one computer can be used by all your other devices

02 SHARE FILES

Got a file on one computer that you need to copy to another computer? Sure, you can use a USB key, but that's hardly the most convenient solution. Fortunately, there's a better way with the technology built into Windows and Mac OS X. Thanks to file sharing, you can simply copy documents over the network, saving time and effort.

03 SHARE PRINTERS

It's not just files that you can share, as Windows and OS X will also let you share printers. That means you can buy one decent printer, but print to it from any device on your network. You may even find that your router or NAS device has built-in printer sharing, so you don't need to leave one computer turned on just to print. Simply put, a home



It might be a bit dull on the outside, but a NAS is the easiest way to share files and media over your network

network makes life a lot easier for everyone and means you can share all your kit with everyone in your home.

03 INSTALL A NAS

A network-attached storage (NAS) device is basically a box containing storage that connects to your network. While that image is a little dry, a NAS could just be one of the most useful things that you ever buy.

For starters, it gives your family a single place to store shared files. While file sharing can do a similar job, you have to leave all the required computers on; a NAS is designed to be left on all of the time, giving you always-on storage.

A NAS can do so much more, too. With the vast majority of models, you can turn them into a media server, storing all of your photos, videos and music in one place, which you can then play on any other device on your home network. With the ability to share printers with most models, a NAS device may be just about the most important and useful bit of networking kit that you buy.

04 HOME ENTERTAINMENT

Why leave all your digital pictures, music and videos locked up on computers where you barely see them? With a home network you can free all these files and view them wherever and whenever you want.

A lot of new TVs and Blu-ray players have media streaming built into them, but you can also add streaming music players, and streaming media players where you want to unleash your digital files. We'll show you how to turn your home network into the ultimate entertainment system. We'll even show you how your smartphone or tablet can be used to control everything.

05 SECURITY

If everything you own is connected to the internet, there's more risk if a hacker can infect your computers. Fortunately, we're here to help with a complete guide to internet security. We'll show you how to stay protected, how to avoid scams and even how to track and recover stolen laptops and mobile phones.

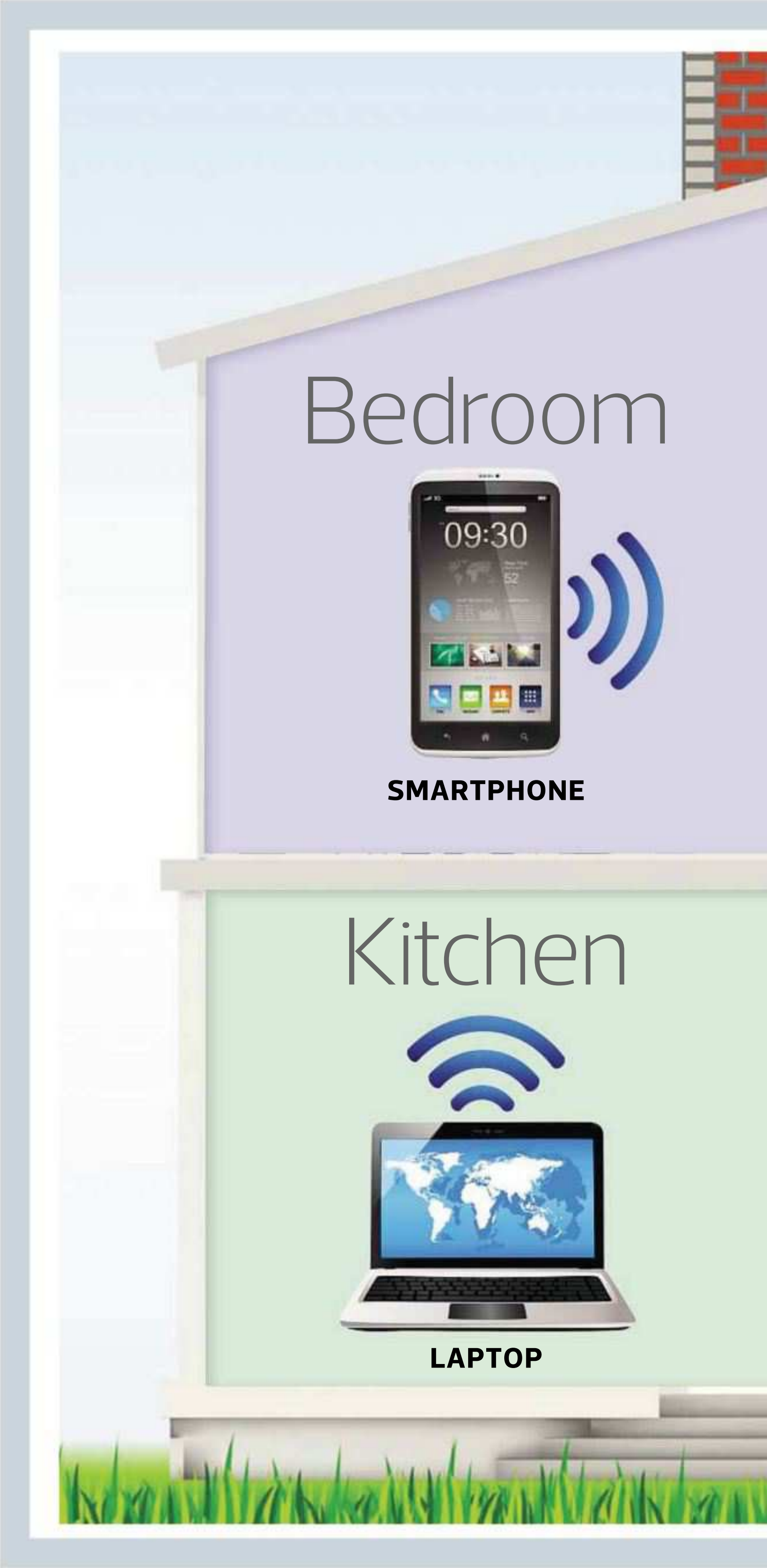
06 THE CLOUD

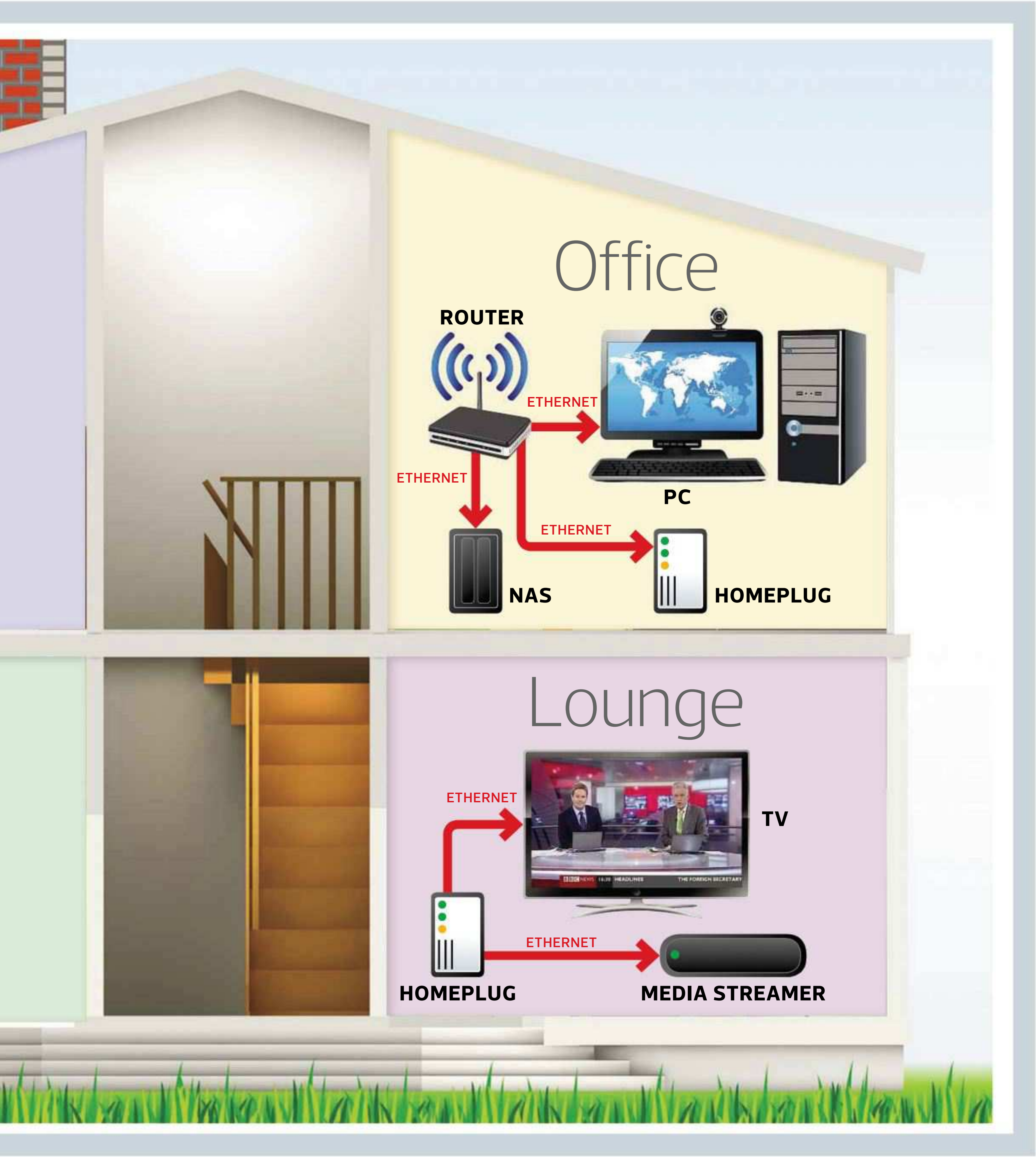
Using cloud storage, you'll find that your internet connection gives you the perfect way to back up and share your files automatically. Unlike other regimes, cloud storage is completely immune to theft, fire and mechanical failure. In other words, it's the simplest and most secure way of ensuring that your precious digital photos, documents, music and videos won't be lost.

With a wireless music player and a NAS, you can listen to what you want, where you want

How to set up a network

This diagram shows a typical house, with the internet coming into the office upstairs. All the devices near the router, such as the desktop PC and NAS device, are connected directly to the router with Ethernet cables. Devices that move (such as smartphones, laptops and so on) are connected by Wi-Fi. Everything else uses HomePlug.




Office
ROUTER
ETHERNET
PC
ETHERNET
ETHERNET
NAS
HOMEPLUG
Lounge
ETHERNET
TV
ETHERNET
HOMEPLUG
MEDIA STREAMER

A wireless router provides everything you need to start your home network

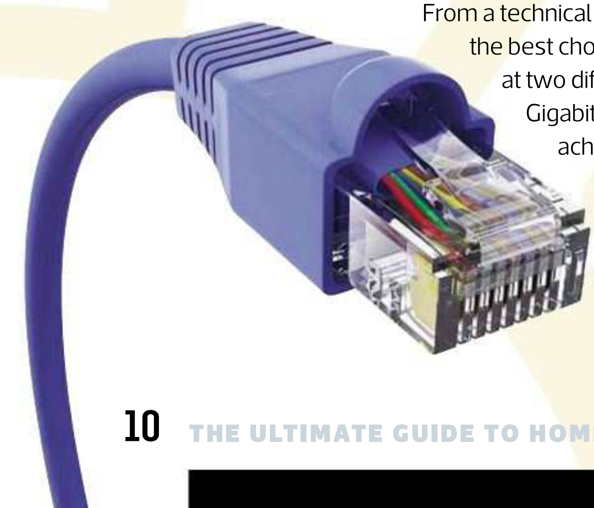
Choosing your kit

There are three main types of technology available for setting up a home network: wireless (Wi-Fi), wired (Ethernet) and powerline (HomePlug), which uses your home's power cables as a wired network. All three are mutually compatible, so using a combination of the three, as we have in our test network *(see diagram, page 8)* will make for the most reliable network. The table *(below)* shows the pros and cons of each networking type, but we'll go into a little more detail here.

Wi-Fi is one of the most convenient ways to set up a network, as the technology is built into the router that provides your internet connection. As it uses radio waves, there's no need to run cables everywhere, and the signal should cover most of a typical house. The downsides are that it's the slowest type of network and can be unreliable, with range being the main problem. The new 802.11ac standard has introduced better speeds, but there are currently few devices that support this standard. We explain how to maximise Wi-Fi range and extend your network on page 25, but even so, wireless is best suited to mobile devices, such as laptops and smartphones. You could connect your PC and other devices wirelessly using USB adaptors, but as they don't move, a more reliable wired connection is better.

From a technical perspective, Ethernet is the best choice for a network. It runs at two different speeds, with Gigabit Ethernet (1,000Mbit/s) achieving the same kinds of transfer speeds as an internal hard disk. Even standard Fast Ethernet (100Mbit/s) is typically faster than most wireless routers. As Ethernet is bi-directional, you technically get twice the bandwidth, as you can simultaneously transmit and receive data at the same speed. It's easy to use, too: plug one end of the Ethernet cable into a router and the other into the device you want to connect, and you're done. However, the practical downside of running cables round your home will outweigh the benefits for many.

Most routers have a four-port Fast Ethernet switch built in, which allows you to connect up to four devices running at



Ethernet is the fastest network connection available

NETWORK MATRIX

This table shows the relative benefits of each

NETWORKING TYPE	QUOTED SPEED
Gigabit Ethernet	1,000 1Gbit/s
Ethernet	100 100Mbit/s
Wireless	300 300Mbit/s (1.3Gbit/s 802.11ac)
HomePlug	500 500Mbit/s

HomePlug devices make it easy to set up a fast, stable network

100Mbit/s at once. A switch is a network device that creates a dedicated connection between two communicating devices (like a telephone exchange), allowing full-speed communications. In contrast, wireless and powerline networks share bandwidth, so the entire speed of the network is shared between all the computers. Gigabit Ethernet and Fast Ethernet are compatible with each other, with the device and router negotiating the connection speed.

You can add Gigabit Ethernet to an existing network by using a dedicated Gigabit Ethernet switch (a five-port model will cost you around £20). Simply connect one port on this to a port on your existing router. Plug all your Gigabit devices into the Gigabit switch and they'll communicate with each other at full speed. This is only worth doing, however, if you copy a lot of large files over your network.

The main downside of Ethernet is that, to use it all over your home, you must install dedicated wiring. This can be difficult and expensive, so Ethernet is mainly suitable for devices near your router, or in situations where you can run a single cable into a room that contains multiple devices, then use a switch to connect them all.

If you don't want to wire up your house for Ethernet, powerline networking is a great choice. This uses your home's electrical mains wiring as network cables, bringing the benefits of a wired network without any rewiring. The technology uses network adaptors that plug into your power sockets. You then connect your devices to these adaptors with Ethernet cables.

HomePlug is the only standard worth using; there are many products available, from single connectors to multiport adaptors. The current HomePlug AV standard runs at a theoretical 500Mbit/s, but in practice you're likely to see transfer speeds of around 93Mbit/s. Faster 500Mbit/s devices are appearing, though *(see page 111)*. Bandwidth is shared between all the HomePlug devices that use the network, so the more you have, the slower the network becomes.

type of networking technology to help you choose the best for each device

TYPICAL SPEED	PROS	CONS	WHAT'S IT GOOD FOR?
850Mbit/s	Extremely fast; easy to use; very reliable	Wiring up the house can be difficult and expensive; not built into many routers	NAS devices; other devices that are close to the router
85Mbit/s	Fast; easy to use; very reliable	Wiring up the house can be difficult and expensive	Devices that are close to the router
50Mbit/s (200Mbit/s 802.11ac)	Built into router; gives you access from anywhere; lets you move easily	Suffers from interference; speeds drop off at distance	Devices that you want to move around your home
93Mbit/s	Fast; reliable; easy to connect devices in different rooms	Comparatively expensive	Fixed devices that are in a different room to the router

Network basics

GETTING STARTED

Our diagram of a typical home network *(see page 8)* will help you work out the best way to network your home. Before you get started, however, it's worth running over some networking basics to help you understand how everything fits together.

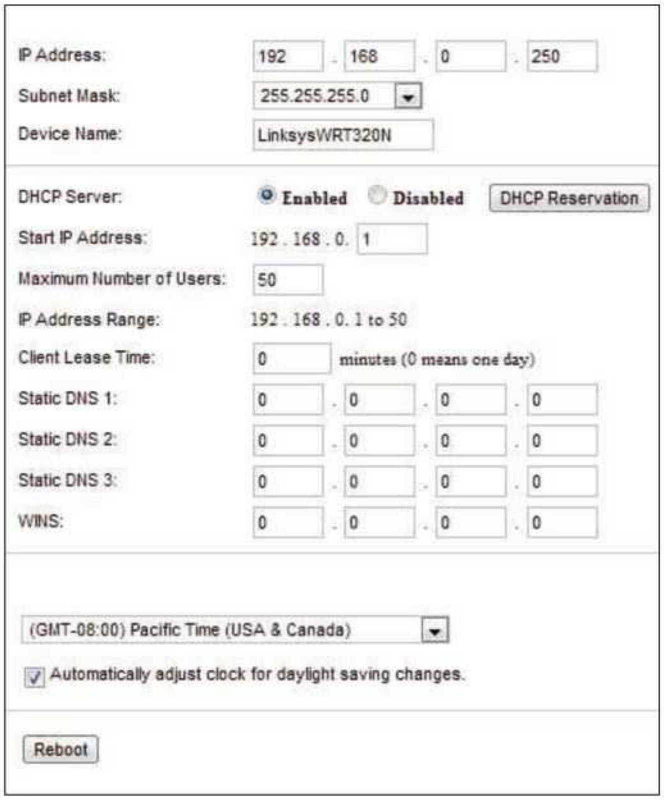
If you don't already have a wireless router, the first thing you need to do is to buy one. These devices are designed to share your broadband connection with multiple computers, and they're an essential part of any home network. Wireless routers provide both wireless and Ethernet networking, and they take a lot of the hassle out of networking. For example, every wireless router has a built-in Dynamic Host Configuration Protocol (DHCP) server. This may sound like a horrific bit of networking jargon, but it means any computers connected to the router will be given an IP address automatically.

Understanding how IP addresses work is an essential part of getting to grips with home networking. You can think of an IP address as your computer's unique postal address on the network. Each computer needs an IP address before it can send and receive data to and from other devices. Without DHCP, you'll have to give every device that connects to your network an address manually; DHCP does it all automatically for you in the background, so you don't need to worry about it.

MANUAL ADDRESSES

The downside of using DHCP is that a device's IP address may change. This is fine for a PC, but for a shared device such as a printer or NAS device, you really need a fixed IP address, which you assign manually. This is why it's important to know how IP addresses work.

> "Wireless routers provide both wireless and Ethernet networking, and they take a lot of the hassle out of networking."



IP Address:	192 . 168 . 0 . 250
Subnet Mask:	255.255.255.0
Device Name:	LinksysWRT320N
DHCP Server:	● Enabled ○ Disabled DHCP Reservation
Start IP Address:	192 . 168 . 0. 1
Maximum Number of Users:	50
IP Address Range:	192 . 168 . 0. 1 to 50
Client Lease Time:	0 minutes (0 means one day)
Static DNS 1:	0 . 0 . 0 . 0
Static DNS 2:	0 . 0 . 0 . 0
Static DNS 3:	0 . 0 . 0 . 0
WINS:	0 . 0 . 0 . 0

(GMT-08:00) Pacific Time (USA & Canada)

☑ Automatically adjust clock for daylight saving changes.

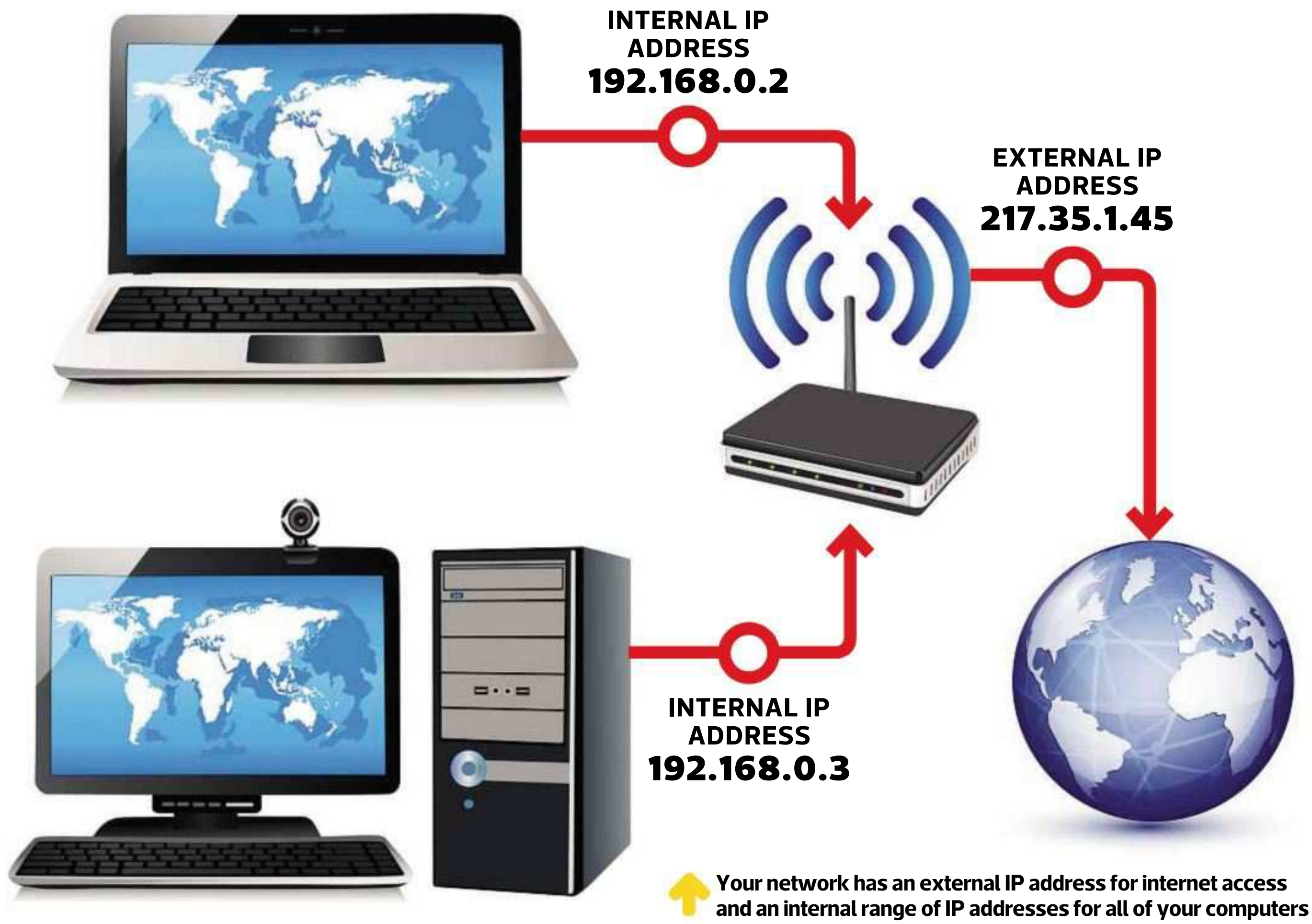
Your router's configuration pages will show you the range of IP addresses it's handing out

On your home network, every device that connects to the router receives an IP address. This is a group of four sets of numbers separated by fullstops, such as 192.168.0.1 or 192.168.0.2.

For devices to be able to talk to each other, they need to be on the same network, which means that the first three sets of numbers of an IP address must be the same. Your router will have a default for this, and it's easiest to leave this alone. The last number is unique for every device on your network. The only rule is that the last number must be between 1 and 254.

Routers are set to dish out only a certain number of IP addresses. Any valid addresses outside this range can be

NETWORKING WITH IP



Your network has an external IP address for internet access and an internal range of IP addresses for all of your computers

given out manually, as the router will never accidentally assign one of them to another computer.

To check this range of IP addresses, you need to access your router's web configuration pages *(see 'Setting Up A Wireless Router' on page 18 for more details on accessing the DHCP part of the configuration screen).* These are usually either in the Basic Setup tab or under Local networks. The range of IP addresses can be defined in two ways: as a start address and an end address (192.168.0.1 and 192.168.0.50, for example), or as a start address and a maximum number of addresses (such as 192.168.0.1 and 50 – in which case, the end address would also be 192.168.0.50). Any address outside this range (excluding the router's own address) can be assigned manually.

When setting a manual IP address, you must also configure a subnet mask, which is 255.255.255.0. This setting is for segmenting business networks, so there's no need to go into it here. Finally, you have to configure a DNS address (again, this isn't worth explaining in detail here), which is simply your router's IP address. Consult the walkthrough on page 18 if you're not sure what it is.

EXTERNAL IP ADDRESSES

As well as an internal IP address, your router has an external IP address that's visible on the internet and is assigned by your ISP. The computers on your network share this address using a technology called Network Address Translation (NAT). An advantage of this is that computers outside your network can't connect directly to any of your computers, which offers a basic level of security from outside attacks. However, you'll have to configure the router for port forwarding if you want to access services on your network, such as an FTP server on a NAS device, over the internet. We'll cover this topic later on.

TP-LINK
Wireless On/Off
USB1
USB LED
USB2

2

CONFIGURING YOUR HOME NETWORK

Getting the perfect reliable home network means choosing the right kit and configuring it all properly. In this chapter we'll take you through everything you need to know, including choosing a new wireless router, working out where you use wired networking and setting everything up. We'll also show you how to improve and extend the range of your wireless network.

CONTENTS

Choosing a wireless router

The type of wireless router you buy depends on your internet connection. If it's ADSL, you'll need a model with a built-in ADSL2+ modem. If you have a fibre-optic network connection, such as BT Infinity or Virgin Media, you'll need a standard wireless router with an Ethernet Wireless Area Network (WAN) port. That said, with a fibre-optic service, you may want to stick with the router you're given: Virgin Media's Super Hub has a built-in cable modem while BT's HomeHub 3.0 is configured to work with your BT Infinity connection. You can disable wireless on the Super Hub, turning it into a modem, so you can connect any WAN port router; it's possible to get these working with Infinity, too.

We've listed our Best Buy routers below to help make your decision easier. You must also decide whether you want a 5GHz or 2.4GHz router. Both types have a maximum throughput of 300Mbit/s (450Mbit/s on some models), but they use different frequencies. Routers that run at 2.4GHz can suffer from interference. In the 5GHz band, there's nothing to interfere with your network except other networks nearby. There are also more wireless channels to choose from, so you can leave channel bonding switched on. It's rare to find an 802.11n wireless router that supports both 2.4GHz and 5GHz networks simultaneously, so 2.4GHz is best for most people.

However, a brand-new 802.11ac wireless router supports both 2.4GHz and 5GHz bands simultaneously and offers much better performance. With a device that supports 802.11ac networking (a growing number do), you can get actual speeds of up to 300Mbit/s, vastly beating standard wireless.

ROUTERS BEST BUYS

802.11ac WIRELESS ROUTER
TP-LINK
AC1750
£102

ADSL WIRELESS ROUTER
TP-LINK
TD-W8980
£75

CABLE ROUTER
TP-LINK
TL-WDR3600
£65

Finally,
a cloud of your own.

Setting up a wireless router

Your wireless router may already be configured when you buy it, but it's worth checking the settings to make sure it's set up correctly. Make a note of these, as you never know when you might have to set up your network from scratch. If you're using ADSL, you'll need to plug an ADSL microfilter into every telephone socket – otherwise, your broadband will cut out every time you make a phone call. However, if you have a replacement master socket face plate with a microfilter built in, you won't need individual filters, as your phones are already filtered from the ADSL connection. With a fibre connection, you don't need additional equipment for your phones, although you'll probably have a separate modem and wireless router.

STEP 01 CONNECT YOUR ROUTER

If you have a fibre-optic internet connection, connect the WAN port on the router to the Ethernet port on the modem using an Ethernet cable. For ADSL connections, you need to use an RJ45 lead. Connect this to the WAN port on the router and the ADSL port of the microfilter plugged into your phone socket or the one built into the face plate.

STEP 02 PLUG IN A PC OR LAPTOP

Next, use an Ethernet cable to connect your laptop or PC to the router. It's possible to configure a wireless router over a wireless connection but it's not a reliable method, so we don't recommend it. With all the devices connected, turn on your wireless router, then turn on your computer and boot into your operating system.

STEP 03 CONNECT TO THE WIRELESS ROUTER

To connect to your wireless router, you need to know its IP address. The router's manual should tell you this, but there's another easy way to find it out. Open a Command Prompt from the Start menu (just type command prompt into the search bar).

When it opens, type ipconfig and hit Enter. Note down the address listed under 'Default Gateway' and type this into a web browser. Your router's login page will appear. Enter your username and password as set by you or documented in the router's manual. This will give you access to the router's web interface, which will probably present you with multiple pages of settings.

01

02

The foundation of business network uptime

APC by Schneider Electric Smart-UPS units protect 24/7/365 network availability.

Safeguarding critical networking switches and routers

Your business depends on your business network. Protecting that network, therefore, is more critical than ever. Known for their reliability for over 25 years, APC™ by Schneider Electric Smart-UPS™ uninterruptible power supplies eliminate costly downtime by providing reliable, network-grade power over a wide range of utility conditions. They keep employees connected to business-critical applications whether they are in house, at a co-location facility, or in the cloud.

A Smart-UPS model for every need

Whatever your IT needs and configuration, we have the right Smart-UPS model. The family offers multiple form factors (tower, rack optimized, and rack/tower convertible) to deliver flexibility for any environment. And you can scale runtime to business requirements. In addition, you can proactively manage the network closet remotely and optimize energy use through a patented "green mode" on many models. Deployment is easy with optional Schneider Electric installation services. Smart-UPS backup units: the intelligent choice for your business network!

Business-wise, Future-driven.™

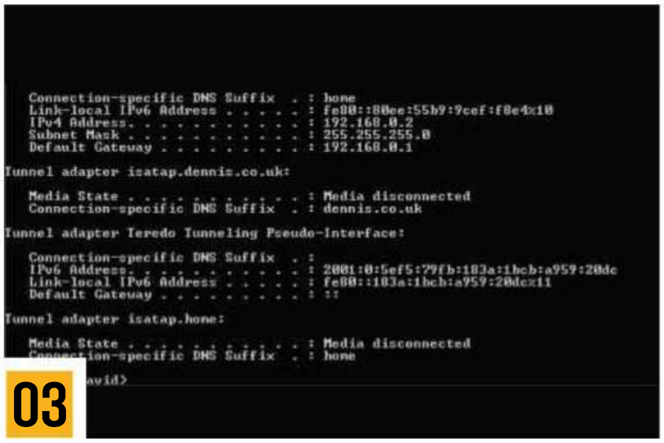
Intelligent battery backup

- **Avoid costly power problems** by keeping your IT equipment and data safe and available with network-grade power conditioning.
- **Reduce operating and maintenance** costs with a patented green operating mode for high efficiency and intelligent battery management that prolongs life and alerts well in advance of replacement.
- **Save time** with easy and convenient remote accessibility, safe operating system shutdown, and innovative energy management.
- **Achieve smarter productivity** by tailoring a variety of settings, including switched outlet control, to your application needs via the intuitive LCD interface or software.

Reduce human-error downtime too!
Get guidance in our FREE white paper and stand a chance to WIN an iPad mini!

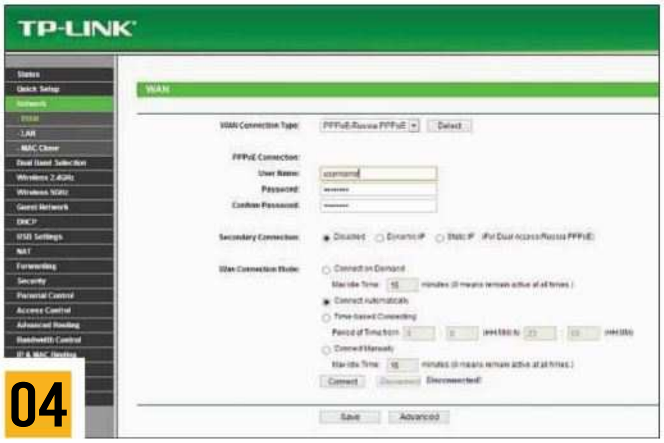
Visit: www.apc.com/promo Key Code: 39426p
Call: 08 45 080 5034 Fax: 0118 903 7840

APC™
by Schneider Electric



03

```
   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::80ee:55b9:9cef:f8e4%10
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.dennis.co.uk:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : dennis.co.uk

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fb:183a:1bcb:a959:20dc
   Link-local IPv6 Address . . . . . : fe80::183a:1bcb:a959:20dc%11
   Default Gateway . . . . . . . . . : ::

Tunnel adapter isatap.home:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home

avid>
```



04

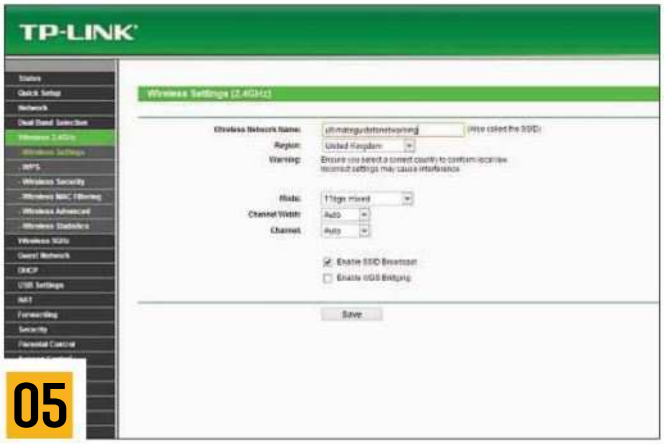
WAN Connection Type: PPPoE/Russia PPPoE [Detect]

PPPoE Connection:
User Name: username
Password: ••••••••
Confirm Password: ••••••••

Secondary Connection: ● Disabled ○ Dynamic IP ○ Static IP (For Dual Access/Russia PPPoE)

Wan Connection Mode: ○ Connect on Demand
Max Idle Time: 15 minutes (0 means remain active at all times.)
● Connect Automatically
○ Time-based Connecting
○ Connect Manually
Max Idle Time: 15 minutes (0 means remain active at all times.)
[Connect] [Disconnect] Disconnected!

[Save] [Advanced]



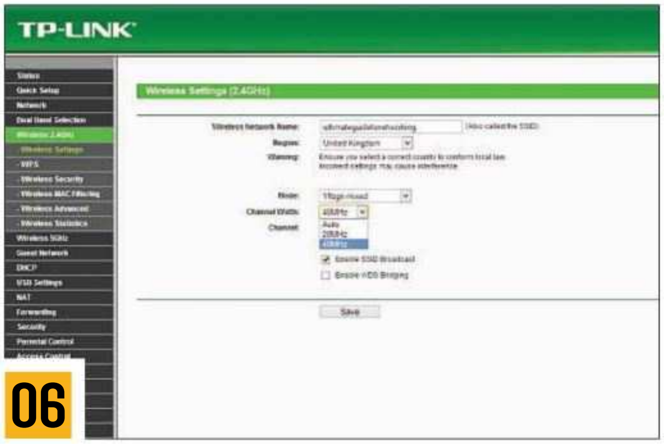
05

Wireless Network Name: ultimateguidetonetworking (Also called the SSID)
Region: United Kingdom
Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode: 11bgn mixed
Channel Width: Auto
Channel: Auto

☑ Enable SSID Broadcast
☐ Enable WDS Bridging

[Save]



06

Wireless Network Name: ultimateguidetonetworking (Also called the SSID)
Region: United Kingdom
Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode: 11bgn mixed
Channel Width: 40MHz
Auto
20MHz
40MHz
Channel:

☑ Enable SSID Broadcast
☐ Enable WDS Bridging

[Save]

STEP 04 ENTER ACCOUNT DETAILS

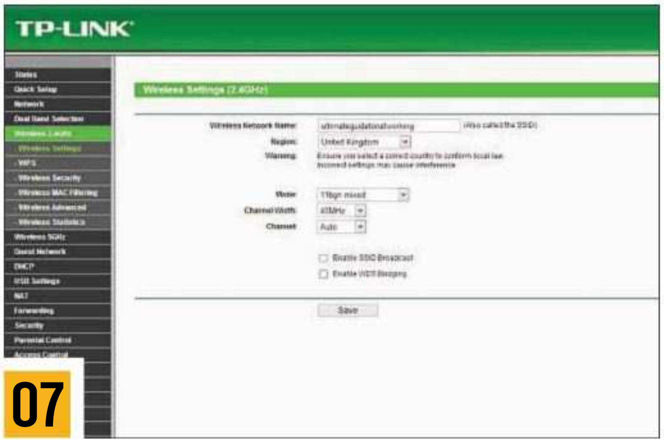
On the internet settings page, enter the account details you received from your ISP. These may include a username and password and, for ADSL connections, advanced options such as Encapsulation. If you can't find these details in the documentation you received when you subscribed to your broadband service, you'll need to contact your ISP. Most cable internet connections don't require you to enter a username and password into the router, so as long as you have a working internet connection, don't worry if these spaces are blank.

STEP 05 CONFIGURE YOUR NETWORK

To configure your wireless network, click on the wireless settings link. The first step is to enter a name for your network. The option might be labelled Name, SSID or ESSID. Type in a memorable name, but for security pick something that doesn't identify you or your house. Next, select the wireless channel. This setting may be on a different page, under a link called Advanced Wireless Settings or something similar. Only use channels that don't overlap (such as 1, 6 or 11), as these don't interfere with each other, and your neighbours will be grateful. You can also configure a 5GHz mode if your router supports it. If your router can only do one band at a time, set 2.4GHz; if not, configure 5GHz, giving it a different name to the first network.

STEP 06 If you have an 802.11n router, disable channel bonding by changing the wireless mode from running at 300Mbit/s (or 270Mbit/s on some routers) to half this speed. This reduces conflict with other networks and is worth doing for 2.4GHz networks. For 802.11ac routers, you can leave the 2.4GHz settings as they are. For routers running at 5GHz, you can leave the fastest setting in place, as you won't have any problems with interference.

STEP 07 If you want to hide your wireless network from casual snoopers, disable your router's SSID broadcast. Doing this will stop your network being listed automatically when a device, such as a laptop or smartphone, is searching for a wireless network. We strongly recommend against hiding your network, though, as it makes it harder to connect devices to your computer and it won't deter a determined attacker, who'll be able to find your network anyway. You may also see an option for Wireless Isolation. This prevents wireless devices communicating directly with other wireless devices on the



07

TP-LINK

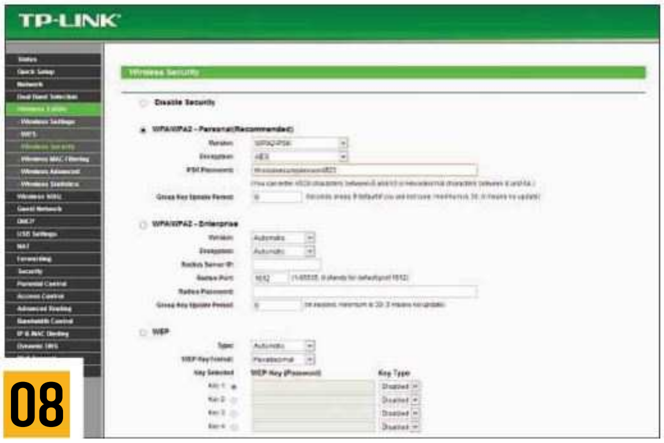
Wireless Settings (2.4GHz)

Wireless Network Name: ultimateguidetonetworking (Also called the SSID)
Region: United Kingdom
Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode: 11bgn mixed
Channel Width: 40MHz
Channel: Auto

□ Enable SSID Broadcast
□ Enable WDS Bridging

Save



08

TP-LINK

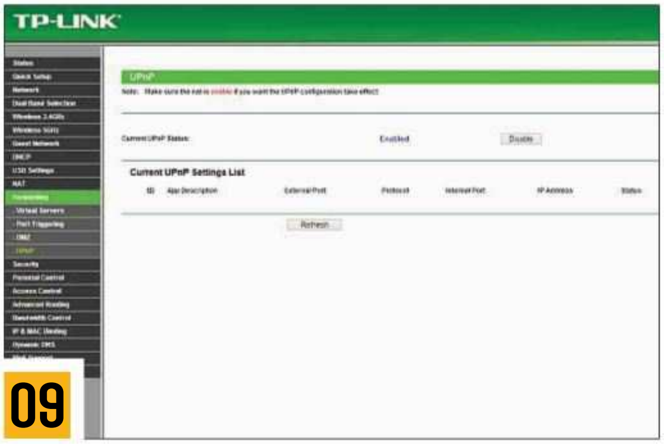
Wireless Security

○ Disable Security

● WPA/WPA2 - Personal(Recommended)
Version: WPA2-PSK
Encryption: AES
PSK Password: [illegible]
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

○ WPA/WPA2 - Enterprise
Version: Automatic
Encryption: Automatic
Radius Server IP:
Radius Port: 1812 (1-65535, 0 stands for default port 1812)
Radius Password:
Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

○ WEP
Type: Automatic
WEP Key Format: Hexadecimal
Key Selected | WEP Key (Password) | Key Type
Key 1: ● | | Disabled
Key 2: ○ | | Disabled
Key 3: ○ | | Disabled
Key 4: ○ | | Disabled



09

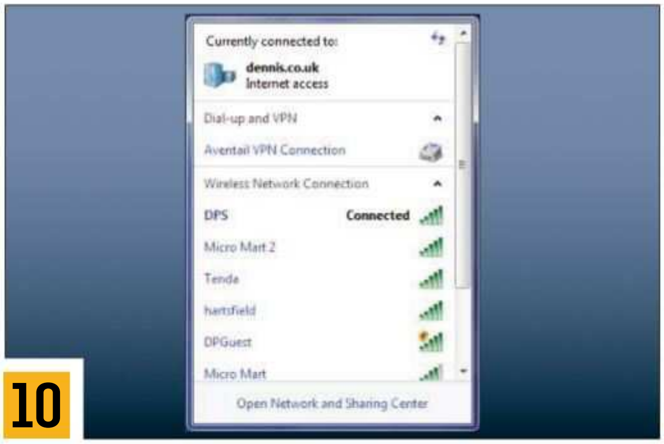
TP-LINK

UPnP
Note: Make sure the nat is enable if you want the UPnP configuration take effect!

Current UPnP Status: Enabled Disable

Current UPnP Settings List
ID App Description External Port Protocol Internal Port IP Address Status

Refresh



10

Currently connected to:
dennis.co.uk
Internet access

Dial-up and VPN
Aventail VPN Connection

Wireless Network Connection
DPS Connected
Micro Mart 2
Tenda
hartsfield
DPGuest
Micro Mart

Open Network and Sharing Center

network. This is useful if you're running a wireless hotspot and you want to give people an extra level of security, but for home use turning it on will make useful activities such as file sharing between wireless computers impossible.

STEP 08 ENCRYPT YOUR NETWORK

Unless you have devices that don't support modern encryption or you're using an older router, select WPA2 encryption in the Security section. Failing that, opt for WPA2/WPA mixed mode. Avoid WEP encryption, as it's insecure and difficult to use – it requires the use of long hexadecimal keys that are hard to remember. Next, enter a password (sometimes called a network key). Choose something that's easy to remember but hard to guess. This is all the security you need, as there's no easy way for anyone to break WPA2 encryption.

STEP 09 ENABLE UPnP

The UPnP technology found on many wireless routers enables your computer to configure the router's firewall automatically, so that it allows through specific services such as video calls in Skype. For the most secure environments, UPnP should be disabled, but for most home networks it should be switched on, as many popular programs and services need it in order to work properly. The location of the UPnP setting varies between routers, but you can usually find it either in an Advanced or Firewall sections of the web interface or by clicking on a dedicated UPnP link.

STEP 10 CONNECT YOUR PC TO THE NETWORK

Save the router's settings and let it reboot. You're now ready to connect your PC to the wireless network. We'll assume that you're using Windows' built-in wireless network software. If additional software came with your network adaptor, its manual will show you how to use it or disable it so you can use Windows' software instead.

In Windows XP, double-click on the icon of a computer with radio waves coming out of it in the Notification Area at the bottom-right of the screen. In Windows Vista, click on the icon with two monitors in the Notification Area, and select 'Connect to a network'. In Windows 7 and 8, click on the network icon for a list of networks. In all operating systems, pick your network from the list. This should have the name you gave it earlier. Click Connect and, when prompted, type in the password you set. Your computer will connect to the network .

Wired networking

For devices that don't move around, we recommend wired networking. It's possible to run Ethernet cable throughout your home – Ethernet cables can be up to around 100m long – but it's a big job, and doing it neatly can be expensive. Unless you can easily take up the floorboards to run network cables underneath, we recommend using an alternative network technology, such as powerline, which routes network signals through your mains wiring.

The most popular technology standard for doing this is HomePlug. Most of these devices comes in three speeds: 85Mbit/s equipment is now old and obsolete, so avoid it. HomePlug AV-compliant products come in speeds of 200Mbit/s, which are great value, and the faster 500Mbit/s products. All products are compatible with each other, so you can mix and match. You can even get HomePlug adaptors with built-in Wi-Fi to extend your network (more on that later).

For devices within easy reach of your router, connecting them couldn't be easier. Simply plug one end of an Ethernet cable into the device and the other into a spare port on the router. The router and the device will negotiate the connection speed automatically.

HOMEPLUG

For HomePlug devices, configuration is fairly simple. Plug the HomePlug adaptor into a wall socket (for the best performance, do this directly rather than through a multi-plug socket). Then plug an Ethernet cable into the HomePlug adaptor and a spare port on your router. The same applies to other devices you want to connect to your HomePlug network. Simply plug another HomePlug adaptor into a socket near the device, and hook up the Ethernet cable.

HomePlug makes wired networking simple and convenient

All HomePlug adaptors of the same standard can communicate with each other by default, but they're not secured as standard. It's possible that neighbours with HomePlug adaptors could end up on your network. To fix this, you need to enable security.

First, it's a good idea to check the manufacturer's website for each HomePlug adaptor to find out if a firmware upgrade is available to ensure compatibility. These can solve security compatibility problems and make a network more reliable.

With push-button security, you simply press the button on one adaptor, then go to the next adaptor and push its button to create a secure network. To add a third adaptor, press the security button on either of the first two adaptors, then press the security button on the third adaptor. Repeat until you've added all your adaptors.

Unfortunately, we've experienced problems with push-button security. If you can't get it to work, try plugging adaptors into adjacent plugs before using the push-button security option. Then, leaving one adaptor plugged in, swap the second one for another and repeat until you've secured them all.

Push-button security is a quick way to add encryption

SECURITY SOFTWARE

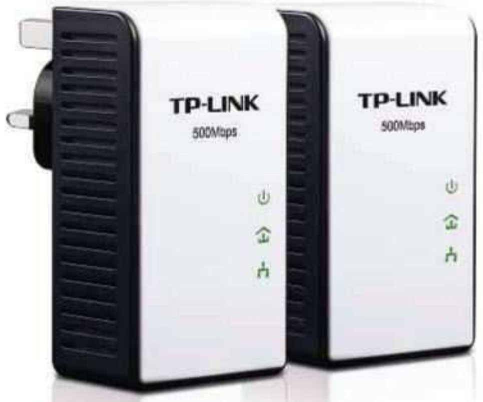
If your HomePlug devices won't connect, you'll have to set them up manually using the utility provided with the devices. Manufacturers ostensibly use compatible utilities, but we've had problems where a manufacturer's utility recognises only its own adaptors. As such, you may need to install each manufacturer's utility. You can download these from the manufacturers' websites.

The utilities look slightly different but work in roughly the same way. Plug an adaptor into a power socket near your computer and connect an Ethernet cable from the adaptor to your computer. Run the adaptor's HomePlug utility. Look for the security option and enter a password of your choice. Then switch adaptors and utilities as necessary until all the adaptors are configured.

In theory, you can configure adaptors without being directly connected to them, but our method is more reliable. Now connect all your adaptors to their sockets and devices, and your network should be fine. If you're buying HomePlug kit from scratch, stick to one manufacturer for the sake of compatibility.

HOMEPLUG BEST BUYS

500Mbit/s KIT
TP-LINK
TL-PA4040PKIT
£40



SUPERFAST 500Mbit/s KIT
TP-LINK
TL-PA511KIT
£45

200Mbit/s KIT
TP-LINK
TL-PA2010KIT
£25

QNAP

Simple yet Powerful NAS

Turbo NAS TS-421

Access your data anywhere

Access your files & enjoy music collection with your mobile devices.

Dropbox like feature - Qsync

Sync your data on your computer, phone, and tablet with the new Qsync.

* TS-421 is featured with the new QTS 4.0 Turbo NAS operating system. QTS 4.0 is also available on TS-x12, TS-x69, and TS-x20 series.

QNAP SYSTEMS, INC.

www.qnap.com

SCAN computers | ebuyer.com | dabs.com | amazon.co.uk

Extending and improving wireless

THE TROUBLE WITH 2.4GHz

Most Wi-Fi networks (802.11n and 802.11ac) operate on the 2.4GHz frequency, as do most 802.11n devices. This frequency is also used by a host of other wireless devices, so as a result it's pretty congested. Baby monitors, DECT cordless phones, Bluetooth headsets, gaming controllers and other wireless PC peripherals all use the 2.4GHz part of the radio spectrum, as do microwave ovens – and they can all interfere with a Wi-Fi signal.

If your Wi-Fi network suffers from slow speeds or connection problems, the first step is to check for potential interference from other wireless devices. Simply moving your router may be enough to remedy the situation, or you may need to accept that you can't use your laptop in the kitchen while microwaving a jacket potato.

The indoor range of a Wi-Fi network can also be affected by the building materials in your home. Wood, plaster and glass have little effect on 2.4GHz radio waves, but brick and concrete can impede them and metal can stop them completely. If your router is mounted on an interior brick wall or sitting on a metal shelf, moving it could improve your signal.

CHOOSING A CHANNEL

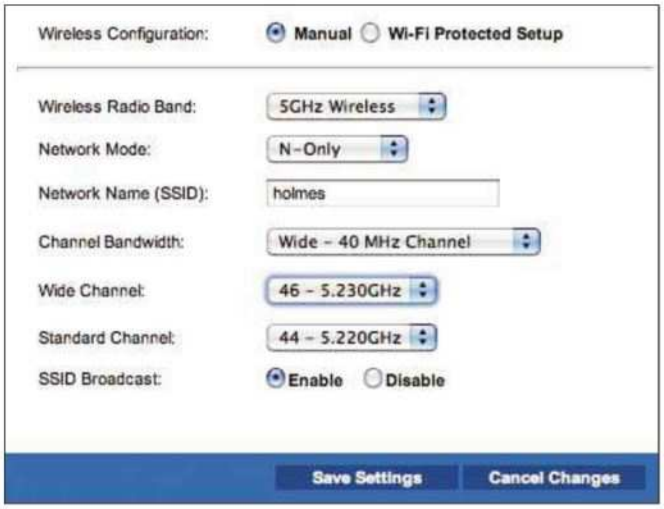
The other major cause of Wi-Fi interference is the presence of other nearby networks. Residential Wi-Fi is everywhere these days, and it's not uncommon to see several other routers when scanning for networks in your own home. Wi-Fi is split across different channels to minimise interference in these situations, but it's usually impossible to ensure that every network is configured appropriately.

The first step in establishing whether nearby networks are causing problems is to conduct a site survey. Using Windows to look at the list of available Wi-Fi networks will give you some idea of which other networks surround you, but this won't show their channel or signal strength.

For this, you need a utility such as the free NetStumbler for Windows (www.netstumbler.com). So equipped, you can wander around your home, noting the channel numbers for any nearby Wi-Fi networks with strong signals (weak networks aren't worth worrying about).

Wi-Fi in the UK is split across 13 channels in the 2.4GHz band (two more than in the US), but you can't just pick a 'free' channel to avoid interference. Channels 1 to 11 are only 5MHz apart, while 12 and 13 are 12MHz apart. As each channel is around 22MHz wide, there's a fair amount of overlap across the channel range, as you can see in our diagram over the page. As a result, only a handful of three-channel combinations can be used without overlap: 1, 6 and 11; 2, 7 and 12; 3, 8 and 13 and so on.

If you manage more than one Wi-Fi network, you can use a complementary channel combination to avoid cross-network interference. If you can't get nearby network owners to do



Wireless Configuration: ● Manual ○ Wi-Fi Protected Setup

Wireless Radio Band: 5GHz Wireless

Network Mode: N-Only

Network Name (SSID): holmes

Channel Bandwidth: Wide - 40 MHz Channel

Wide Channel: 46 - 5.230GHz

Standard Channel: 44 - 5.220GHz

SSID Broadcast: ● Enable ○ Disable

The 5GHz band offers up to 19 UK channels with no overlap the same, the only option is to set your Wi-Fi router's channel so that it has as little overlap with the other networks as possible – or so that at least it only overlaps with the weaker networks. Take care when choosing channels 12 and 13, though. In theory, any Wi-Fi router approved for use in the UK should support them, but not all laptop Wi-Fi adaptors do.

FIX INTERFERENCE WITH 5GHZ

If your Wi-Fi network uses only 802.11n or 802.11ac devices, you may have a better way to avoid interference. The 802.11n and 802.11ac specifications can also operate at 5GHz, which is far less congested. Better still, 5GHz's 19 UK channels (not all of which are available on all routers) have no overlap, which makes it much easier for nearby networks to coexist.

If your Wi-Fi router is 'dual-band', it can use the 5GHz band; look for the appropriate option under the Wi-Fi settings in its web interface. Unless your router supports simultaneous dual-band Wi-Fi, though, switching to 5GHz will mean that 802.11b/g devices are unable to connect. Not all 802.11n Wi-Fi adaptors support 5GHz, either, so turning off 2.4GHz will cut those off, too (the iPhone 4 falls into this category).

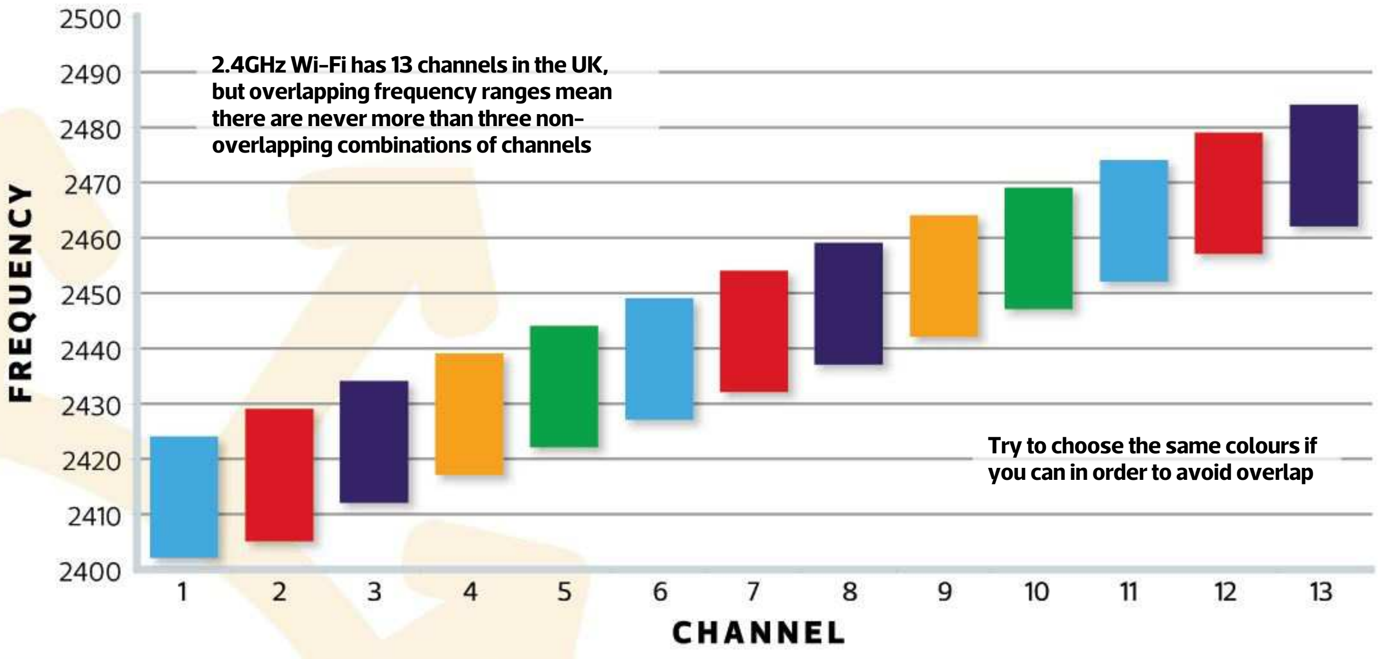
> “Ultimately, there's a limit to how far your wireless network can reach, no matter where you place the router.”

The only other snag with 5GHz is that it doesn't have quite the same range as 2.4GHz Wi-Fi, as its higher-frequency radio waves can't penetrate solid objects as effectively. This may not matter for most homes, but it's worth thinking about if you can't get a strong signal.

DOUBLE UP

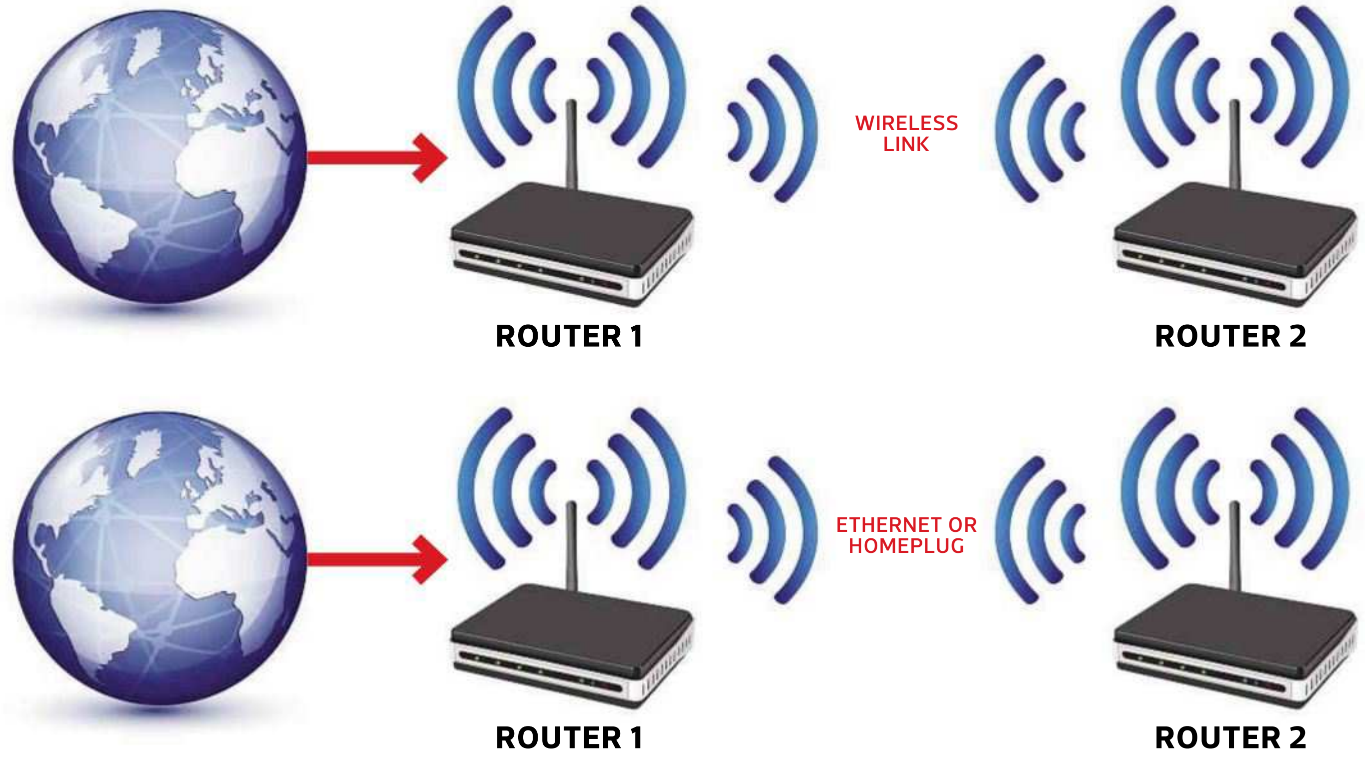
If you have an 802.11n router, whether it's 2.4GHz or 5GHz, there's an option for a Wide Channel. This uses an additional wireless channel to double the throughput. In fact, the 300Mbit/s headline speed of 802.11n assumes that two

CHOOSING A CHANNEL



EXTENDING WIRELESS RANGE

If you want to extend your wireless range, try linking one router to another



channels are used. This technique, known as channel bonding, should be avoided on 2.4GHz 802.11n networks. This radio spectrum is already overcrowded, and sapping up another radio channel just doubles the interference. It's not just for the sake of your neighbours, either: channel bonding can cause all kinds of interference problems that stop your network working. 802.11ac networks are smarter, so channel bonding is fine.

For 5GHz 802.11n networks, the channels don't overlap and there are more of them. As such, channel bonding isn't so bad, so turn it on and see if it boosts your speeds. If you run into stability problems, disable it again.

EXTENDING YOUR WIRELESS RANGE

Ultimately, there's a limit to how far your wireless network can reach, no matter where you place the router. If you need better coverage, you'll need to install a second wireless router. There are several ways to do this. One of the ways promoted by wireless router manufacturers is to use the Wireless Distribution System (WDS).

With this method, you place the second router close to the wireless black spot and use WDS to connect it wirelessly to the first (*see diagram, above*). WDS requires a compatible router – we recommend the cheap TP-Link WR702N router (£19 from amazon.co.uk). This method avoids the need for any more wiring, but you're adding an extra wireless link, which can make for a slow and often unreliable connection.

> “You can buy HomePlug adaptors with built-in wireless access points that do the same job and are more convenient.”

A better method is to connect the first wireless router to the second over an Ethernet or HomePlug connection. This gives you a much more stable link and better performance, and you don't need WDS-compatible equipment. Alternatively, you can buy HomePlug adaptors with built-in wireless access points that do the same job and are more convenient.

For any of these methods to work, you need to set up the second wireless router correctly. Start by following the steps on page 18 for setting up a wireless network. Use the same settings you used for your first wireless network, but pick a different channel that doesn't overlap.

Next, go to the second router's DHCP settings page and disable DHCP (if you don't, the router will hand out a mess of IP addresses and nothing will work). Finally, change its IP address manually to a static address that's in the right range for your main network. Save the settings.

You're now ready to connect the two routers, either by Ethernet or HomePlug. For a simple wired connection, use a long Ethernet cable to hook up a spare Ethernet port on your main router to a spare port on your second router. For HomePlug, connect a spare port on your main router to the HomePlug adaptor, and then plug in a second HomePlug adaptor near your second router and connect the two with an Ethernet cable. Do not use the second router's WAN port.

You should now have wireless everywhere in your home. As you move around, your wireless devices will switch seamlessly to the strongest wireless signal. You'll see only one network, and you shouldn't need to adjust any settings on your devices.

If you need to change your wireless network settings, you'll need to do this on both routers. You'll also need to connect to the second wireless router using the IP address that you gave it earlier. Using this method, you'll find that wireless will be more reliable everywhere in your home. ■

WIRELESS EXTENDERS BEST BUYS

WIRELESS POWERLINE EXTENDER
TP-LINK
TL-WPA4220KIT
£75

WIRELESS ROUTER/RANGE EXTENDER
TP-LINK
WR702N
£19

WD
My Cloud

CHAPTER 3

3

SHARING FILES AND PRINTERS

One of the best things about having a network is that it makes it easy to share things between your computers. In this chapter we'll look at how you can share files between your Windows and Mac computers, and even share printers. With our advice you won't have to hunt for a USB key ever again.

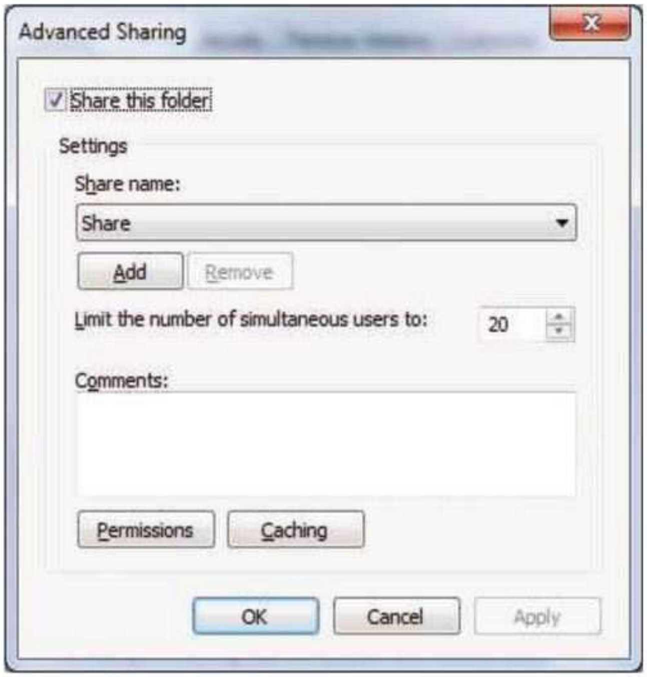
CONTENTS

Sharing files

The ability to share files and folders is a key part of Windows networking. In this chapter we'll show you how to do this, and also look at configuring Windows 7 and 8 so that they work with older operating systems, as well as Mac OS.

SHARING FILES

Sharing a folder in Windows is easy. Simply find the one you want to share in Explorer, right-click it and select Properties, then click the Sharing tab. Finally, click the Share button to make the folder available on the network. However, some system folders, such as the Windows directory, can't be shared and will have the necessary button greyed out.



Advanced Sharing

☑ Share this folder

Settings

Share name: Share

Limit the number of simultaneous users to: 20

Comments:

If you don't want to share a particular folder, go to Advanced Sharing options

In Vista, Windows 7 and Windows 8 you need to select which users you want to give access to it over the network. In XP, usernames aren't required, as the default allows read-only sharing, but you can select the 'Allow network users to change my files' option for read\write access. In Vista, Windows 7 and Windows 8, the default shared username will be listed in the main window, along with a Permission Level of Owner. You should leave this setting alone, but choose additional users that will have access to this folder.

If you turned off password-protected sharing, you should select the Guest account from the drop-down menu and click Add. If you're using password-protected sharing, select the user accounts that you want to allow access and click Add; repeat for as many user accounts as you need. To give all user accounts access, select Everyone from the drop-down menu.

Next, for each account you've selected, you can choose the Permission Level. Read lets users look at, but not modify, files stored in this folder, while read/write allows users to view and modify files in the folder. For home use, it's best to set read/write as the permission level for all users, unless you don't want network users to be able to modify files.

When you've finished, click the Share button, then Done, and your folder will be available on the network. If you want to change who has access to a shared folder, right-click on it in Explorer, click Properties, select the Sharing tab and then click the Share button.

You can add new users using the instructions above, and remove existing users' access by changing the Permission Level to Remove. Click the Share button again to make your changes. To stop sharing a folder completely, go back to the Sharing tab and click Advanced Sharing. Remove the tick from the 'Share this folder' option and click OK.

ACCESSING SHARES

You can now access any shared folders you've created from other computers. Your Windows machine should appear when you browse the network from another PC using Explorer. In Windows XP, open an Explorer window and expand My Network Places, Entire Network and Workgroup. You should see the other computers on your network. Select them to view shared files. In Vista, expand Network and Workgroup, then select your other computers. In Windows 7 and Windows 8, expand Network to do the same thing.

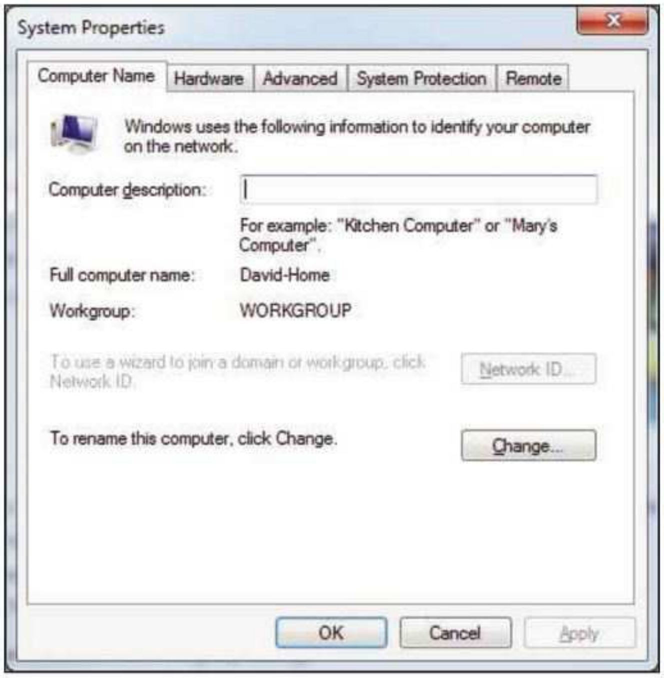
If you can't see your computer, you can connect to it directly from a remote machine. To do this, press Windows-R to bring up a run command. Type '\\<name of your Windows PC>' and press OK; you can also type in the name of your NAS device or any other computer. If you don't know the name of your Windows machine, you can find it by right-clicking on Computer in its Start menu and selecting Properties. Click the 'Advanced system settings' link and then the Computer Name tab. Your machine's name will be listed after 'Full computer name'.

Alternatively, you can connect to any shared folder by pressing Windows-R and then typing \\<IP address of device>. You can find out the IP address of a Windows PC by getting a command prompt up and typing 'ipconfig'; for a NAS device, you'll need to check its web interface.

At this point, you might find that you'll be prompted to enter a username and password. Just type in a valid username and password for the device to which you're connecting. To make life easier, you should create matching usernames and passwords on all computers and peripherals; for example, on a NAS device, make sure you have the same username and password as you do on your Windows computer.

You should be wary if you're connecting to a Windows 7 PC. We've had problems trying to use a username with a space in it, such as 'David Ludlow', when trying to connect from a Windows XP computer. This doesn't happen on all machines, and seems to be a problem that's unique to some computers. To get round this, you should create a new username that doesn't use a space in it on your Windows 7 or Windows 8 machine *(see 'Creating user accounts', opposite).*

> “To make life easier, you should create matching usernames and passwords on all computers and peripherals.”



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: David-Home

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer, click Change.

It's easy to find out your computer's name

MAPPING A NETWORK DRIVE

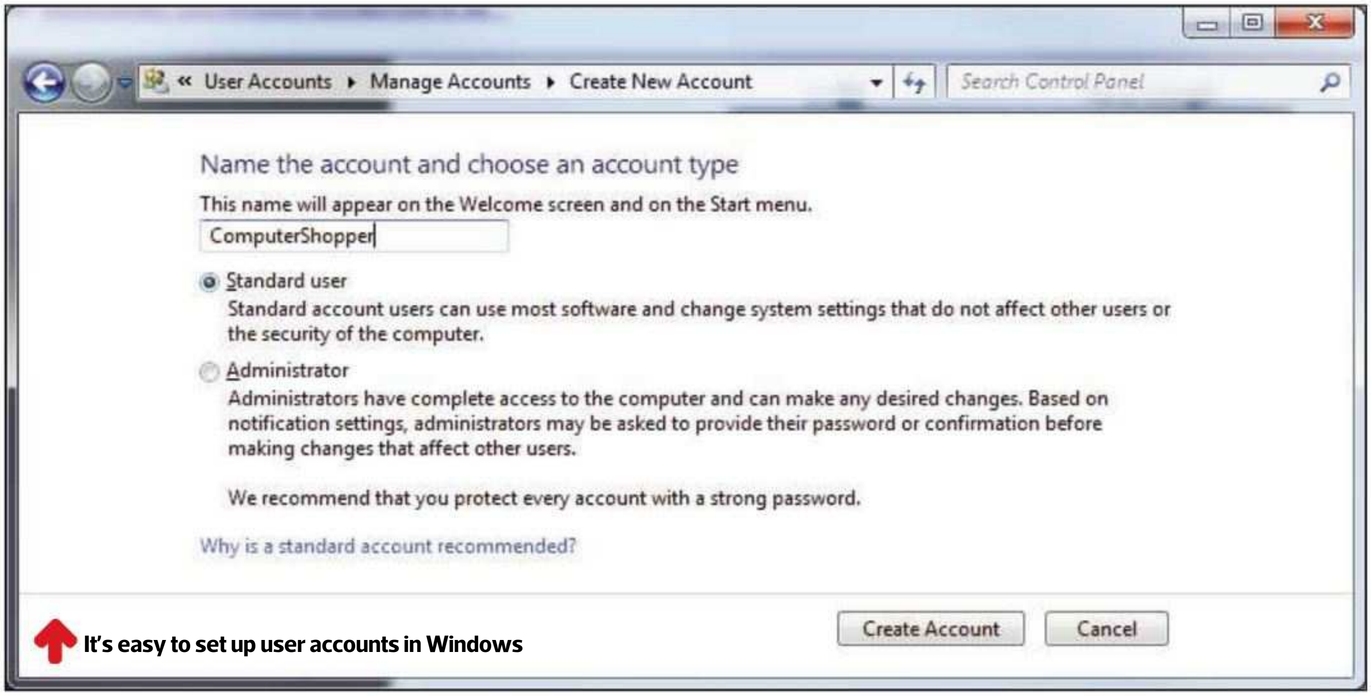
From Windows, it's also possible to create mapped network drives so that you can access a shared folder through Computer as though it were a normal hard disk. Simply right-click on the shared folder you want to access (it must be the root shared folder in this case) and select Map network drive. Choose the drive letter you want to use from the drop-down menu and click Finish when you're done.

CONFIGURING WINDOWS 7 AND 8

Windows 7 and 8 can be picky about what they work with, but a little configuration will soon get it working with older computers and NAS devices on your network.

First, you need to sort out the sharing features. To do this, go to the Control Panel and open Network and Sharing Center. Click on the 'Change advanced sharing settings' in the left-hand panel. Make sure that 'Home or Work' is selected (Private in

CREATING USER ACCOUNTS



Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

ComputerShopper

● Standard user
Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

○ Administrator
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

Why is a standard account recommended?

It's easy to set up user accounts in Windows

Creating user accounts is incredibly simple. In all versions of Windows, select User Accounts from the Control Panel. In Windows Vista, 7 and 8, you'll need to click 'Manage another account', then 'Create a new account'. In Windows XP, you can just click 'Create a new account'.

In all versions of Windows, type the username you want to use. In Vista, 7 and 8, you're given a choice of the type of user account. Opt for Standard if you don't want users to be able to install software or make other system changes. If you want to allow this, select the account type as Administrator. Click Create account. In Windows XP, click Next to get the same choice; note that a Standard account in Windows XP is called a Limited account. Click Create Account when you're done.

Next, you need to configure a password for the new account. Simply click the account you've created and then 'Create a password', and type in the one you want to use. Make sure you use the same account names and passwords in all versions of Windows – otherwise, file sharing won't work properly.

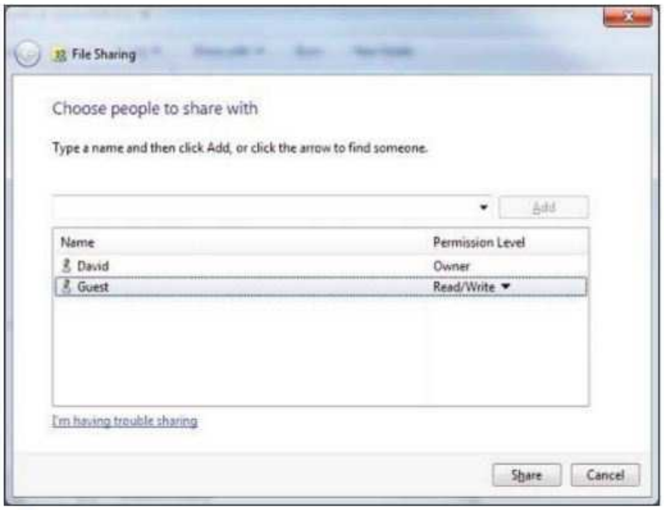
Windows 8) – otherwise, you'll be changing the sharing settings for when you connect to a public network, such as a Wi-Fi hotspot. First, ensure that 'Turn on network discovery' is selected, then click 'Turn on file and printer sharing'. You should be fine with the 'Use 128-bit encryption to help protect file sharing connections (recommended)' option (listed under All Networks in Windows 8), but if you're having trouble after you've followed the rest of our advice, change to 'Enable file sharing for devices that use 40- or 56-bit encryption'.

Finally, you can choose whether you want to require other people to use passwords to access your shares. If you do – and we would recommend it for security reasons – make sure that 'Turn on password protected sharing' is selected (listed under All Networks in Windows 8), but if you want to make things easier, select 'Turn off password protected sharing'. Your computer is now set up to share files.

SHARING WITHOUT PASSWORDS

If you set up Windows 7 or Windows 8 to share your folders without having to use a password, you'll probably be a bit confused if a username and password box pops up when you connect from another computer. Fortunately, this is a simple problem to fix.

The main cause of this issue is that you're using a username on a Windows XP or Vista PC that matches a username on your Windows 7 computer, but with different passwords. Just change the password of the user account on the XP or Vista machine to match the one used on the Windows 7 or 8 computer.



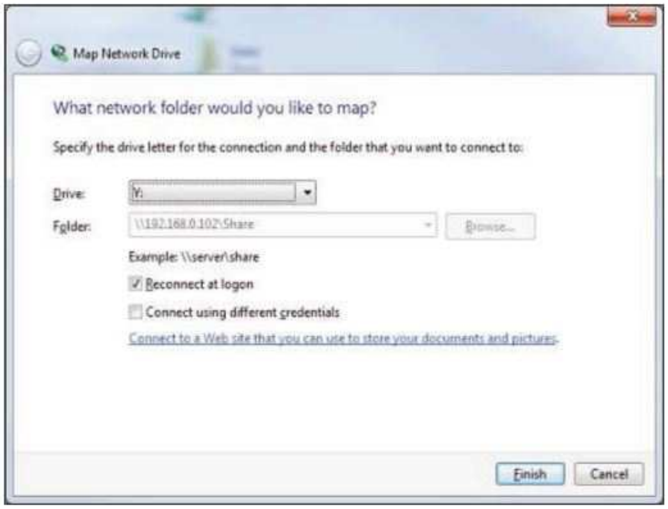
File Sharing

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
David	Owner
Guest	Read/Write ▾

Choose the level of access each user has to a folder



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

Folder: \\192.168.0.102\Share

Example: \\server\share

☑ Reconnect at logon

☐ Connect using different credentials

Browse...
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

You can also map a drive letter to a shared folder

On all Windows operating systems, you'll need to log on using the account that needs a new password. First, press Ctrl-Alt-Delete and click Change password. Enter your old password and then your new password twice and click OK. You should now find that your Windows XP or Vista computer connects to the Windows 7 machine.

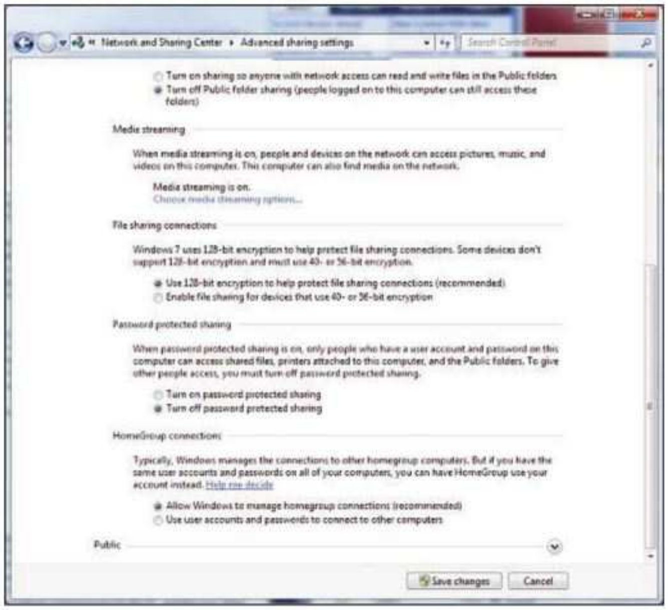
SHARING WITH PASSWORDS

If you set up Windows 7 to require usernames and passwords, you'll need to configure your Windows XP and Vista computers to have the same usernames and passwords. Our guide on the previous page tells you how to do this, but you can change the password for a user account in any version of Windows by pressing Ctrl-Alt-Delete and then clicking Change password. As we mentioned earlier, we've had problems with usernames that have a space in them, so you may need to create usernames and passwords that don't have spaces in them on your Windows XP, Vista and Windows 7 machines.

If you don't use passwords on your user accounts and you're having problems, try creating passwords on them. Don't forget that if you create any new usernames on Windows 7 or 8, you'll need to make sure that this user is set to have access to shared folders.

ACCESSING FILES

You should now be able to access your Windows 7 or 8 machine from Windows XP or Vista, and double-click any shared folder to view its contents. If you've set up read/write access, you'll be able to drag and drop new files into the shared folder. If you can't access a folder, go back to the Windows 7 PC and check the share permissions; make sure the Guest account has access for password-free sharing, and the relevant username has access for password-protected sharing.



Network and Sharing Center ▸ Advanced sharing settings

○ Turn on sharing so anyone with network access can read and write files in the Public folders
● Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Media streaming is on.
Choose media streaming options...

File sharing connections

Windows 7 uses 128-bit encryption to help protect file sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.

● Use 128-bit encryption to help protect file sharing connections (recommended)
○ Enable file sharing for devices that use 40- or 56-bit encryption

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

○ Turn on password protected sharing
● Turn off password protected sharing

HomeGroup connections

Typically, Windows manages the connections to other homegroup computers. But if you have the same user accounts and passwords on all of your computers, you can have HomeGroup use your account instead. Help me decide

● Allow Windows to manage homegroup connections (recommended)
○ Use user accounts and passwords to connect to other computers

Public

You can tell Windows 7 not to require passwords when you're sharing files over your network

From Apple to Zeiss, and everything in between

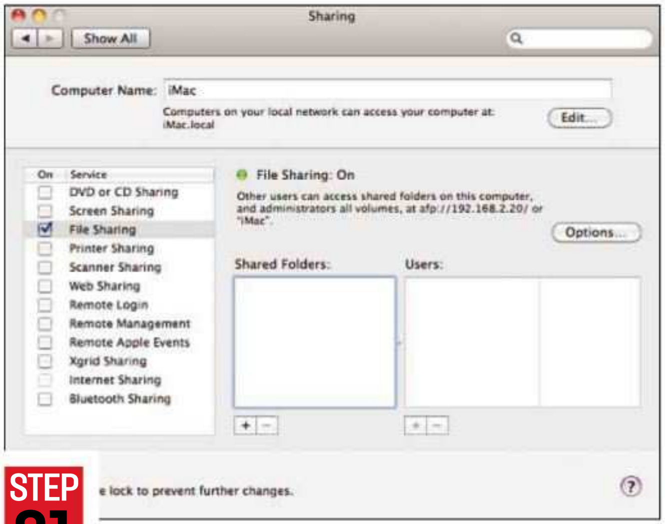
Sharing files between Windows and Mac OS

Sharing removable storage devices between Macs and Windows PCs can be tricky because of their mutually incompatible native file systems. However, things are much easier when the PCs are connected to the same network.

Both operating systems support a file-sharing protocol called SMB, which acts independently of the underlying file system. In other words, as long as SMB access is properly configured, a Mac can access the contents of a Windows PC's hard disk across a network – and vice versa – with the minimum of fuss.

In this walkthrough we'll show you how to share files across different platforms, such as Mac OS X and Windows XP, Vista, 7 and 8, using the standard features of each operating system. The only potential pitfall is that Mac OS X supports a wider range of characters in file and folder names than Windows, and Mac filenames containing a plus sign or an asterisk, for example, will confuse a Windows PC.

We'll be using computer names to access network shares, because they never change – unlike the dynamic local IP addresses usually used by home networks. Computer names are easier to remember and identify, too, although IP addresses can be a more reliable way of connecting to a remote computer. So, if you have problems connecting to a remote Mac or PC using its name, you can simply substitute its IP address – smb://iMac might become smb://192.168.1.18, for example. You'll see the Mac's IP address for share access in the dialog box for Step 2, but for Windows machines, you'll need to use 'ipconfig' again to find it.



Computer Name: iMac

Computers on your local network can access your computer at: iMac.local

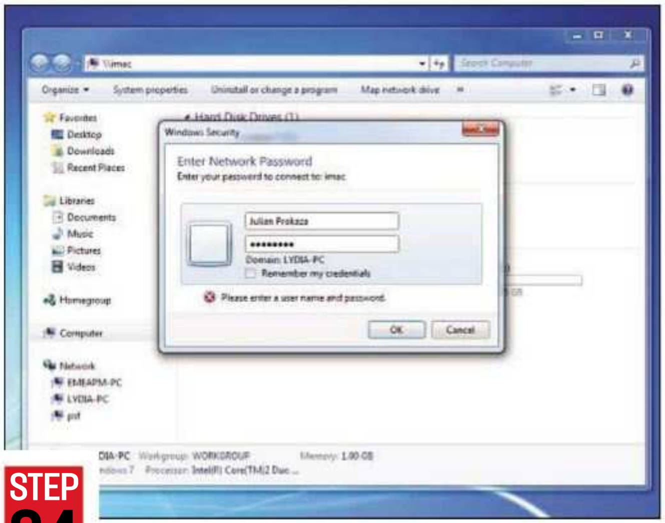
On	Service
□	DVD or CD Sharing
□	Screen Sharing
☑	File Sharing
□	Printer Sharing
□	Scanner Sharing
□	Web Sharing
□	Remote Login
□	Remote Management
□	Remote Apple Events
□	Xgrid Sharing
□	Internet Sharing
□	Bluetooth Sharing

● File Sharing: On

Other users can access shared folders on this computer, and administrators all volumes, at afp://192.168.2.20/ or "iMac".

e lock to prevent further changes.

STEP 01 To access files stored on a Mac using Windows, start by setting up file sharing on the Mac. Select System Preferences from the Apple menu, then click Sharing. When the dialog box opens, ensure that an easily identifiable computer name is provided in the field at the top and that file sharing is enabled in the column of services on the left. Click to select the File Sharing service, then click the '+' button below the Shared Folders field to browse for a folder to share.



Windows Security

Enter Network Password

Enter your password to connect to: imac

Julian Prokaza

•••••••••

Domain: LYDIA-PC

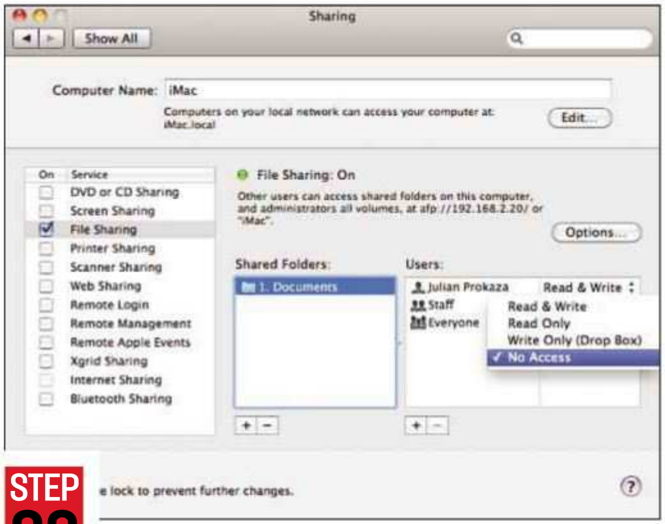
□ Remember my credentials

Please enter a user name and password.

DIA-PC Workgroup: WORKGROUP Memory: 1.00 GB

ndows 7 Processor: Intel(R) Core(TM)2 Duo ...

STEP 04 To access the shared Mac folder from within Windows, open an Explorer window and type \\<computer name> (from Step 1) into the address bar – \\My-iMac, for example. Press Return and then wait several seconds for a connection to be established. You'll then be prompted to enter your Mac username and password, after which you'll have access to your shared folders.


Sharing

Computer Name: iMac

Computers on your local network can access your computer at: iMac.local

File Sharing: On

Other users can access shared folders on this computer, and administrators all volumes, at afp://192.168.2.20/ or "iMac".

On	Service
□	DVD or CD Sharing
□	Screen Sharing
☑	File Sharing
□	Printer Sharing
□	Scanner Sharing
□	Web Sharing
□	Remote Login
□	Remote Management
□	Remote Apple Events
□	Xgrid Sharing
□	Internet Sharing
□	Bluetooth Sharing

Shared Folders: 1. Documents

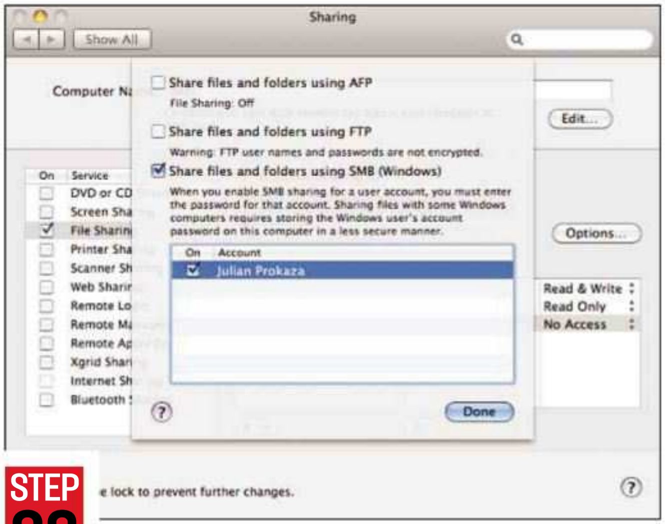
Users:	
Julian Prokaza	Read & Write
Staff	
Everyone	

Read & Write
Read Only
Write Only (Drop Box)
✓ No Access

e lock to prevent further changes.

STEP 02

Once a folder has been selected for sharing, three entries will appear in the Users field alongside it, together with access permissions for each. Only the first user – your Mac login username – is used for file sharing with Windows; the other two can be ignored. You may want to change the access permissions of Staff (all user accounts on this particular Mac, apart from the Guest account) and Everyone (all other Macs on the network), to avoid exposing your files to other Mac users. You can share multiple subfolders rather than one parent folder to help with security; repeat Step 1 for each folder you want to access from Windows.


Sharing

□ Share files and folders using AFP

File Sharing: Off

□ Share files and folders using FTP

Warning: FTP user names and passwords are not encrypted.

☑ Share files and folders using SMB (Windows)

When you enable SMB sharing for a user account, you must enter the password for that account. Sharing files with some Windows computers requires storing the Windows user's account password on this computer in a less secure manner.

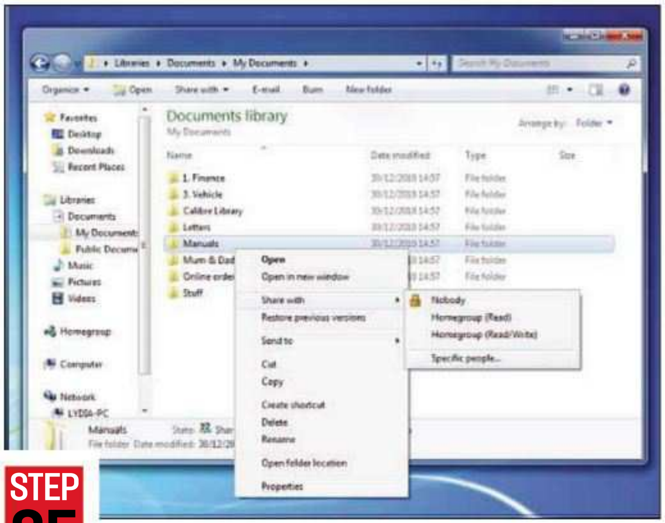
On	Account
☑	Julian Prokaza

Read & Write
Read Only
No Access

e lock to prevent further changes.

STEP 03

With the folders chosen and user permissions set appropriately for each, click the Options... button. When the dialog box appears, enable the 'Share files and folders using SMB (Windows)' option and, if the 'Share files and folders using AFP' option is enabled, disable it, unless you also want to share files across the network with other Macs. You'll also need to enable your Mac user account for SMB sharing in the box below this and confirm by entering your Mac login password. Click the Done button to close this dialog and quit System Preferences.


Libraries ▸ Documents ▸ My Documents ▸

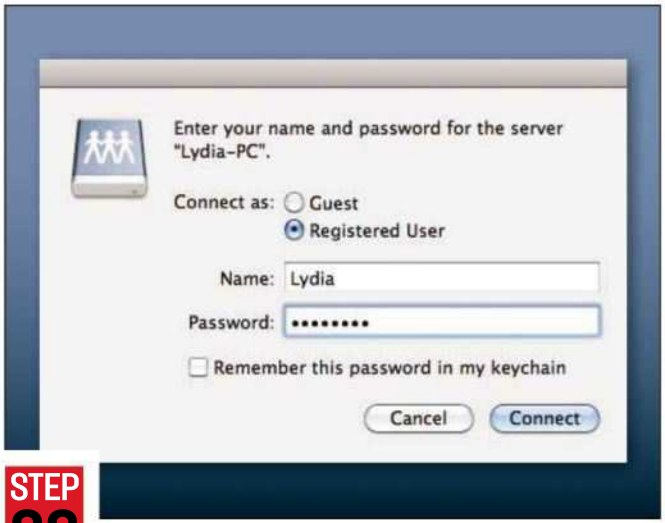
Documents library

My Documents

Name	Date modified	Type	Size
1. Finance	30/12/2010 14:57	File folder	
3. Vehicle	30/12/2010 14:57	File folder	
Calibre Library	30/12/2010 14:57	File folder	
Letters	30/12/2010 14:57	File folder	
Manuals	30/12/2010 14:57	File folder	
Mum & Dad	14:57	File folder	
Online orde	14:57	File folder	
Stuff			

STEP 05

Accessing shared Windows files from a Mac is much the same. You need the Windows PC's name. In Windows XP, Vista and 7, right-click on Computer and select Properties to view it. In Windows 8, press Windows-X and select Properties, click Advanced System Properties and then Computer Name. Next follow the steps on page 33 to share a folder on your Windows computer.


Enter your name and password for the server "Lydia-PC".

Connect as: ○ Guest ● Registered User

Name: Lydia

Password: ••••••••

□ Remember this password in my keychain

STEP 06

To open the Windows share on the Mac, open the Desktop's Go menu and select the Connect to Server option (or press ⌘+K). Enter the server address as smb://<Windows computer name> *(see Step 5)* and click the Connect button. For Vista and 7 shares, you must then enter the username and password for the Windows user account; you can just use Guest for Windows XP (unless you specified otherwise in its share setup). Click the Connect button and the share will be mounted.

Many modern printers have networking built in, making them easy to share with multiple computers

Sharing printers

While we all usually have more than one computer on our networks, we typically only have a single printer. Sharing this on the network is important, as it cuts down on the need for having to copy documents across the network and always using the same PC to print out a document.

A shared printer is also useful for computers that aren't always in the house, such as laptops. Fortunately, sharing printers over a network is easy. However, there are a few ways of doing it, depending on the hardware you have available.

NETWORK PRINTER

A printer with a network port used to be an expensive luxury, but a growing range of consumer models come with both wired and wireless networking. The advantage of this method is that you don't need any other hardware or software to share your printer on the network. As the printer is designed to be a network model, you can usually access all its features, such as the scanner, which aren't always available using the other methods we've listed here. Simply plug in the printer, follow the installation instructions in the manual and install the printer software on any computers you have. If you're looking to buy a new printer and have the budget for it, we recommend that you buy a networked model.

> “A printer with a network port used to be an expensive luxury, but a growing range of consumer models come with both wired and wireless networking.”

NETWORK SHARING

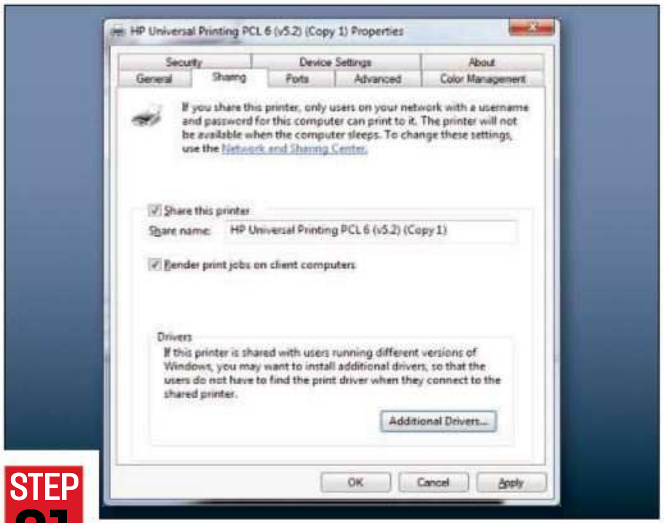
If your router or NAS device has a USB port, there's a good chance that they'll support printer sharing. You'll need to check your manual to make sure before you start. If they do, you have a built-in way of sharing a USB printer over the network, and you don't need to leave a computer turned on.

The disadvantage of this method is that you have to position your printer near your computer. The alternative is to go for a dedicated network print server, which is a small box that turns your USB printer into a network model, usually via a wireless connection. In all three cases, the rough settings are very similar, although you'll need to check your device's manual for the exact settings.

Plug your printer into a network USB port on your chosen device and turn it on. Go to the web-based management page of your

You can share printers using different NAS devices, provided that they have a USB port

SHARING A PRINTER



HP Universal Printing PCL 6 (v5.2) (Copy 1) Properties

If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

☑ Share this printer

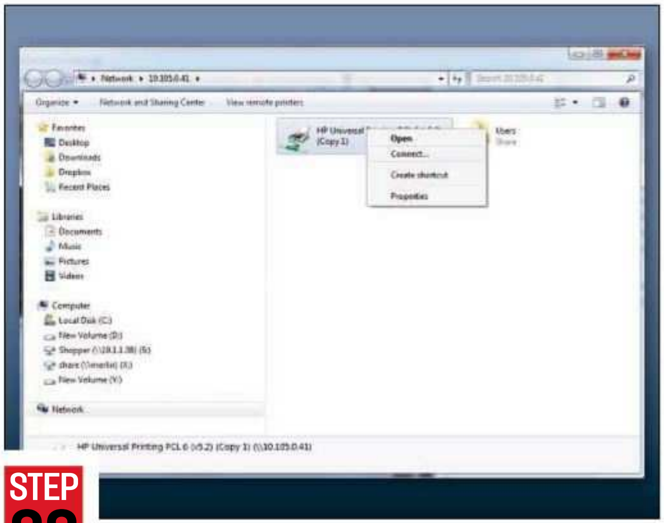
Share name: HP Universal Printing PCL 6 (v5.2) (Copy 1)

☑ Render print jobs on client computers

Drivers

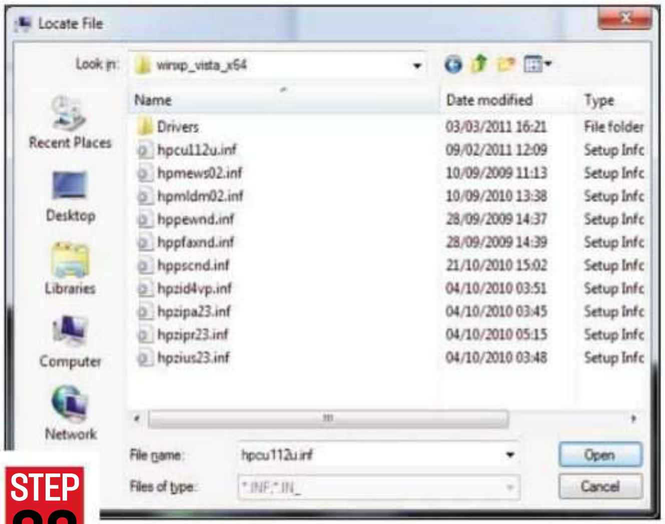
If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

STEP 01 On the computer that has the printer driver installed, go to the Printers section of the Control Panel. Right-click on the printer you want to share and select Properties. Next, click the Sharing tab and select Share this printer; you can change the name of the printer if you like. Click OK to share the printer.



HP Universal Printing PCL 6 (v5.2) (Copy 1) (\\10.105.0.41)

STEP 02 To connect to the printer, go to a different PC. Connect to the computer sharing the printer (Start, Run, \\<IP address of print machine>) and, if prompted, type in a username and password for the computer to which you're connecting. You should now see the shared printer. Right-click on it and select Connect. If the computer you're connecting from is running the same operating system as the printer you're connecting to, it should download and install the print drivers automatically. If it's a different operating system, you'll be prompted to install a driver manually, so go to Step 3.



Locate File

Look in: winxp_vista_x64

Name	Date modified	Type
Drivers	03/03/2011 16:21	File folder
hpcu112u.inf	09/02/2011 12:09	Setup Infc
hpmews02.inf	10/09/2009 11:13	Setup Infc
hpmldm02.inf	10/09/2010 13:38	Setup Infc
hppewnd.inf	28/09/2009 14:37	Setup Infc
hppfaxnd.inf	28/09/2009 14:39	Setup Infc
hppscnd.inf	21/10/2010 15:02	Setup Infc
hpzid4vp.inf	04/10/2010 03:51	Setup Infc
hpzipa23.inf	04/10/2010 03:45	Setup Infc
hpzipr23.inf	04/10/2010 05:15	Setup Infc
hpzius23.inf	04/10/2010 03:48	Setup Infc

File name: hpcu112u.inf

Files of type: *.INF;*.IN_

STEP 03 Download the drivers for your operating system from the printer manufacturer's website. If you can, extract the downloaded file to a folder on your computer; if it's an executable, you'll need to run the installation routine to get the driver on your computer (make a note of where the files are installed). Use the file browser to navigate to the printer's driver (the folder will contain an .inf file) and click Open. Click OK and the printer will be added to your computer. You can then select the remote printer when you print or even set it as the default printer.

router, NAS device or print server, and look for a Printers or External devices section. Your printer should be listed in the list of devices; if it isn't, it's probably not supported by your chosen device.

Select your printer and turn on sharing. You should now be able to view the printer over the network (*see the walkthough above*), although some printer servers require you to install special software on them before you can access the printer.

You should be aware that using this method often means that you can't access an MFP's scanner over the network. Some network print servers offer this functionality, but only on a limited range of MFPs, and it's by no means guaranteed. As such this kind of sharing is best for standard printers. If you need to use a scanner, too, you'll need to go for sharing via your computer.

PC COMPUTER SHARING

Perhaps the easiest way of sharing a printer is to use the file sharing built into Windows. This is free and has the advantage that you can use all your printer's features from the connected computer, although you'll only be able to print from other networked machines. The main disadvantage is that the computer the printer is connected to has to be left on for this to work. ■

WD

4

ADDING STORAGE TO YOUR NETWORK

A network-attached storage (NAS) device is best described as a hard disk in a box with a network connection. While that may sound uninteresting, you can use one as an always-on method of sharing files, a home entertainment server for all your digital media and even a way to access your files remotely. In this chapter we'll show you how to choose, configure and access your NAS.

CONTENTS

Adding a NAS device

An increasing number of homes now have a computer network. However, as any IT manager will tell you, a good network needs a server that acts as a repository for shared files. You can set up one of your home PCs to act as a file server for music, photos and other files, but it would need to be switched on permanently to give your other computers continuous access to the data.

A far better solution is to buy a dedicated NAS device. These are smaller and use less power than a computer, which means they can be left on permanently, providing storage for your computers whenever they need it. Many can also act as print servers, and they make network backups easy, too.

In this chapter, we'll take you through the process of installing a NAS device on your network.

CHOOSING A NAS DEVICE

NAS devices cost more than internal hard disks, but they're still great value. Most provide storage for less than a pound per gigabyte. The simplest products contain a single hard disk, but bigger, more expensive models often have multiple disks. As an alternative to providing more storage space, products with multiple disks can be configured in a RAID array to protect your data if one disk fails.

Even if you can't afford a RAID-enabled NAS device, you can still protect your data. Most models come with USB ports, so you can plug in an external USB disk for quick and easy backups. You may also be able to plug in a USB printer and share it on the network automatically.

> “Some NAS devices have advanced features such as media servers to share files with streaming media players.”

You can buy a NAS device with wired or wireless network interfaces. The former is cheaper and quicker than even the fastest wireless network. If you already have a wireless router, it should have some Ethernet ports, so you'll be able to connect a wired storage device, making it available wirelessly, too. However, we recommend that you spend extra on a wireless storage device only if you don't already have an up-to-date wireless router, or you need to position your file server somewhere you can't easily reach the cables.

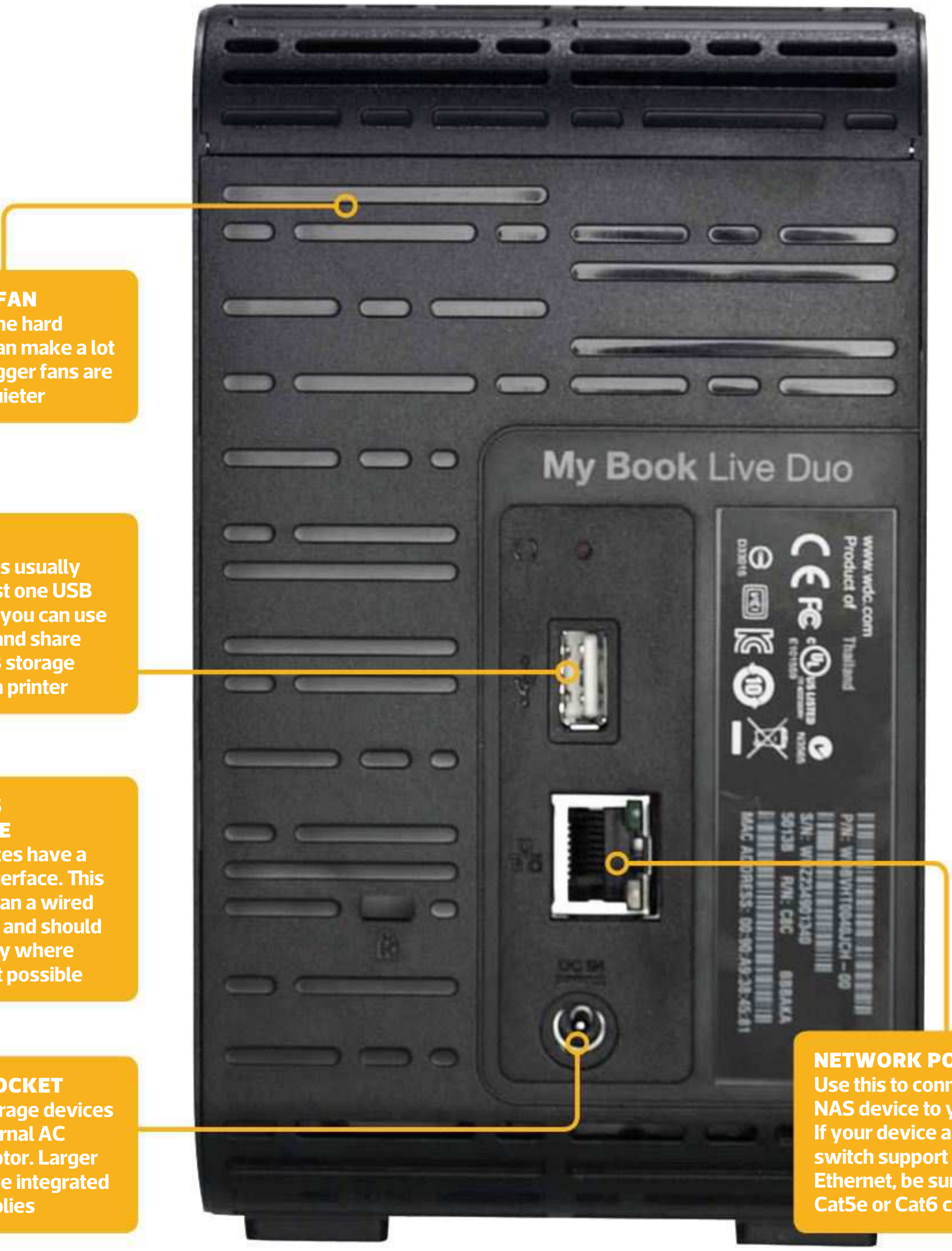
Gigabit Ethernet provides the fastest performance when accessing your network storage, but your NAS device, computers and router or network switch must all support this standard in order to get the quickest speeds. You'll also have to replace any Cat5 Ethernet cables that you have with Cat5e or Cat6 cables for reliably high speeds.

Most NAS devices are designed to be left on all the time. Unfortunately, some – especially those with more than one hard disk – can be noisy, so you may want to tuck them away in a cupboard. You should, however, make sure that there's plenty of ventilation, as some devices can become warm.

Microsoft's Universal Plug and Play (UPnP) protocol is supported by most NAS devices. This means that they can connect to the computers on your network with little or no configuration. Versions of Windows from Me onwards have UPnP support built in, so you won't have any problems getting a NAS device to work on your network.

Those models that don't support Microsoft's standard use their own drivers, setup utilities or web interfaces for installation and configuration. Some of these may have their own requirements, such as a particular version of Windows, so you should check what these are.

Some NAS devices have advanced features such as media servers to share files with streaming media players. This is a brilliant feature and one that lets you use your home



COOLING FAN
This cools the hard disks, but can make a lot of noise. Bigger fans are normally quieter

USB PORT
NAS devices usually have at least one USB port, which you can use to connect and share further USB storage devices or a printer

WIRELESS INTERFACE
Some devices have a wireless interface. This is slower than a wired connection, and should be used only where wires aren't possible

POWER SOCKET
Smaller storage devices use an external AC power adaptor. Larger models have integrated power supplies

NETWORK PORT
Use this to connect your NAS device to your network. If your device and network switch support Gigabit Ethernet, be sure to use a Cat5e or Cat6 cable

network for entertainment. We can't recommend getting a NAS with a media server enough, and we think that it should be a standard part of any home network.

INSTALLATION

The physical installation of a NAS device is comparatively simple and shouldn't cause you any problems. The software you need to install will vary, depending on the version of Windows you use, and the make and model of your device. You may need to install drivers before you attach the device to your network; read the manufacturer's instructions to find out what you need to do.

Our guide on the following pages takes you through the typical setup of a NAS device.

➜

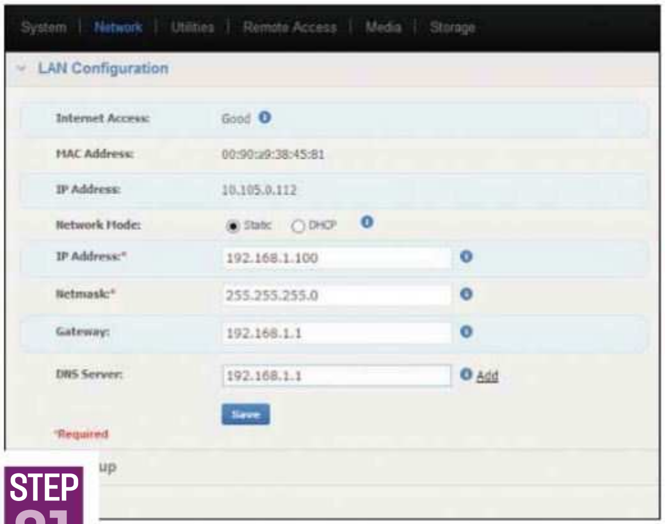
Configuring a NAS device

Every NAS device is slightly different, and you'll need to refer to its manual for exact instructions. However, what we'll teach you to do here applies to the majority of models.

We're using a Synology NAS device for this walkthrough, as it's one of the easiest to configure. We'll be focusing on access over a local network, while on the following page we show you how to access your NAS over the internet.

To configure your device, you'll need to connect to its IP address using a web browser, which you should be able to find in the manual. Alternatively, most models come with a network utility that lets you detect your device on the network, giving you all the information you need.

Once you have your device's IP address, type iy into a browser. You'll need to enter the administrator username and password to make any changes; again, you should find these in the device's manual.


System | Network | Utilities | Remote Access | Media | Storage

LAN Configuration

Internet Access: Good

MAC Address: 00:90:a9:38:45:81

IP Address: 10.105.0.112

Network Mode: ● Static ○ DHCP

IP Address:* 192.168.1.100

Netmask:* 255.255.255.0

Gateway: 192.168.1.1

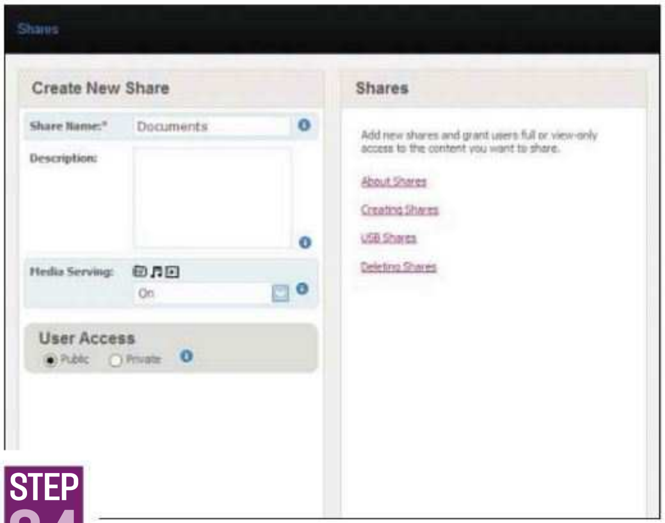
DNS Server: 192.168.1.1 Add

Save

*Required

up

STEP 01 You'll be connecting to your NAS device on a regular basis, so you must make sure you can always find it on your network. The easiest way to do this is to set it up with a fixed IP address *(see Chapter 2)*. First, look for the network configuration setting in the web management page. When you find the relevant setting, change it from automatic IP address (DHCP) to manual. Next, type in the address you want to use. You'll also need to give your NAS device a name, so you can recognise it on the network. When you're ready, save the settings.



Create New Share

Share Name:* Documents

Description:

Media Serving: On

User Access

● Public ○ Private

Shares

Add new shares and grant users full or view-only access to the content you want to share.

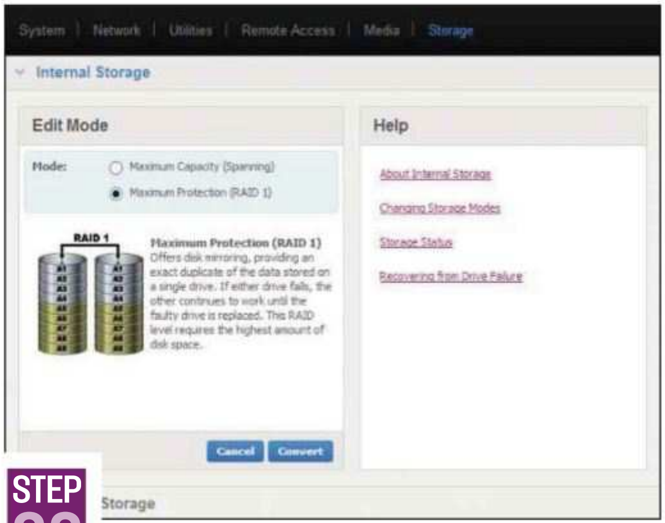
About Shares

Creating Shares

USB Shares

Deleting Shares

STEP 04 You now need to create shared folders. It makes sense to create at least one folder per user if your NAS device doesn't do it automatically. For files you want to share between multiple users, such as videos, pictures and MP3s, it's worth creating a separate folder. The only thing to be aware of is that if your NAS device has a UPnP media server for streaming media, it may already have specified folders for these file types. Find the option to create shares and set up a new one for each user. After you've done so, you may be asked to set file permissions, which we'll cover in the next step. Repeat for as many folders as you need.


System | Network | Utilities | Remote Access | Media | Storage
Internal Storage
Edit Mode
Help
RAID 1
Cancel
Convert
Storage

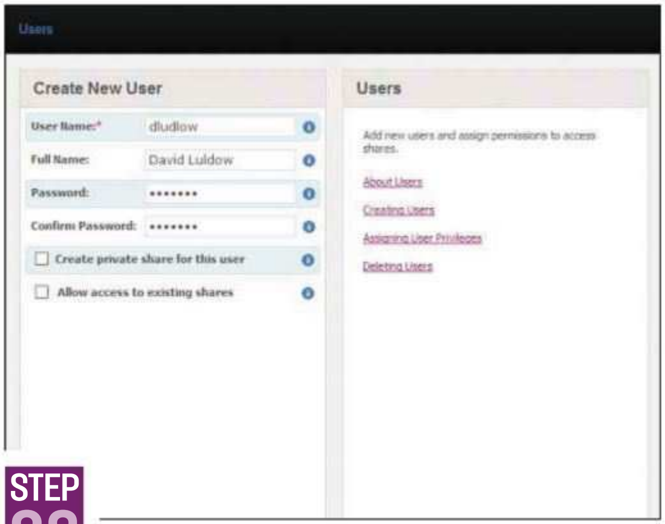
Mode: ○ Maximum Capacity (Spanning) ● Maximum Protection (RAID 1)

Maximum Protection (RAID 1)
Offers disk mirroring, providing an exact duplicate of the data stored on a single drive. If either drive fails, the other continues to work until the faulty drive is replaced. This RAID level requires the highest amount of disk space.

About Internal Storage
Changing Storage Modes
Storage Status
Recovering from Drive Failure

STEP 02

Next, you need to configure your storage device. Look for an option called Storage, Volumes or similar. Click the New Volume (or similar) link to create shared storage space. If you have more than one hard disk, you'll see an option to use multiple disks in a RAID array. For this to work, you'll need disks of the same size. With two disks, you have a choice of RAID 0 (striping), which gives you better performance but no protection, or RAID 1 (mirroring), which halves the storage available but writes all the files to both disks for extra protection. With three or more disks, you can use RAID 5 (parity). For most home users, two disks and RAID 0 is the best option.



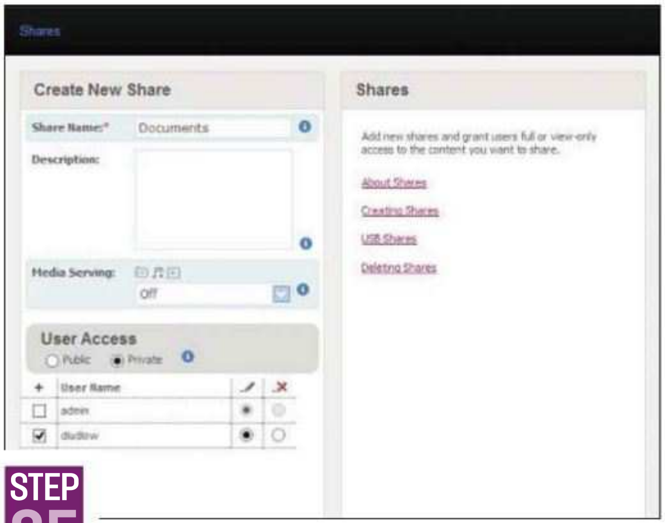
User Name:* dludlow
Full Name: David Luldow
Password: •••••••
Confirm Password: •••••••
□ Create private share for this user
□ Allow access to existing shares

Add new users and assign permissions to access shares.

About Users
Creating Users
Assigning User Privileges
Deleting Users

STEP 03

To configure users, go to the User accounts section of your NAS device. You'll need to create accounts with the same usernames and passwords that you use on your regular computers. That way, you won't have to enter usernames and passwords whenever you connect to a network. If you don't want usernames and passwords, look for a Guest account and make sure that it's enabled. This will allow people to connect without usernames or passwords.



Share Name:* Documents
Description:
Media Serving: Off

○ Public ● Private

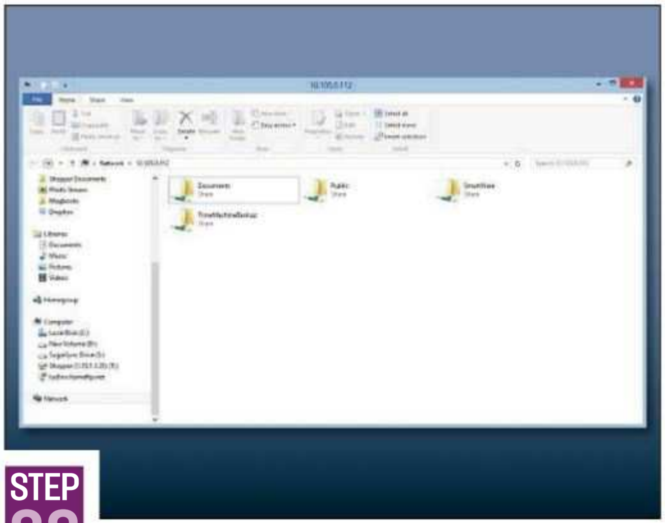
+	User Name	✎	✗
□	admin	●	○
☑	dludlow	●	○

Add new shares and grant users full or view-only access to the content you want to share.

About Shares
Creating Shares
USB Shares
Deleting Shares

STEP 05

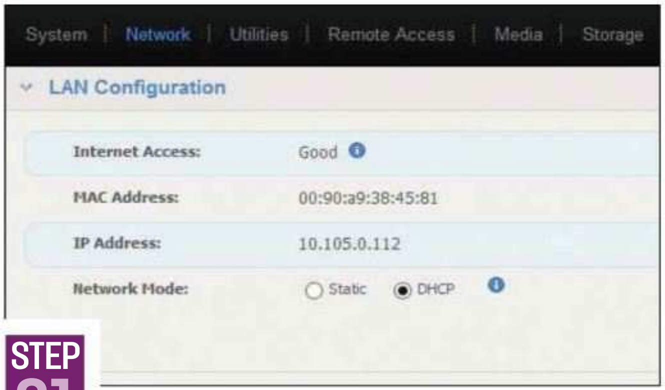
Once you've created your shared folders, you need to set up permissions. This defines which users can access them. You normally have a choice of read-only or read/write for full access. Select the levels that apply for each user. If you don't want to use usernames and passwords, you'll probably need to give the guest user read/write access to the shared folder.



STEP 06

Your NAS device is now ready to use. You can connect to it by pressing Windows-R to get a Run command up, and typing \\<IP address of NAS>, or browsing for the device using Windows Explorer. You can even map a network drive.

How to connect to your NAS device remotely


System | Network | Utilities | Remote Access | Media | Storage

LAN Configuration

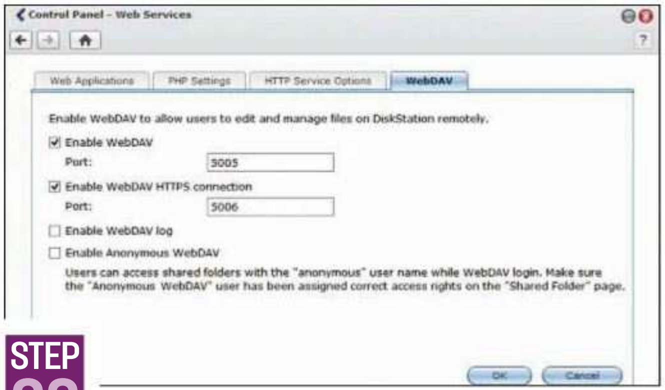
Internet Access: Good

MAC Address: 00:90:a9:38:45:81

IP Address: 10.105.0.112

Network Mode: ○ Static ● DHCP

STEP 01 First of all, you need to turn on any methods of remote access. File Transfer Protocol (FTP) is one such method that is commonly used, and if you have a website this is the method you'll be using to upload files. Connect to your NAS device's web interface and look for the FTP option. Select the option to enable it, and make a note of the port number it's using, as you'll need this later. The default port is 21, and you should change this only if you have good reason to do so.



Enable WebDAV to allow users to edit and manage files on DiskStation remotely.

☑ Enable WebDAV

Port: 5005

☑ Enable WebDAV HTTPS connection

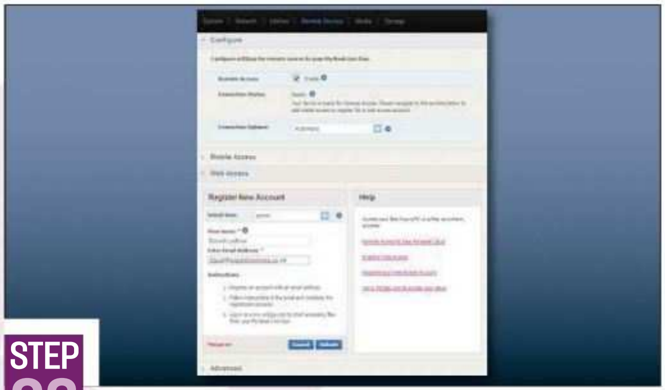
Port: 5006

☐ Enable WebDAV log

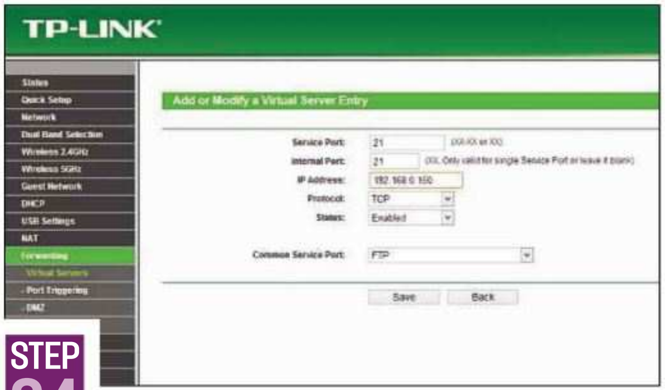
☐ Enable Anonymous WebDAV

Users can access shared folders with the "anonymous" user name while WebDAV login. Make sure the "Anonymous WebDAV" user has been assigned correct access rights on the "Shared Folder" page.

STEP 02 WebDAV is an alternative remote access protocol. For clients that support it, WebDAV lets you access your NAS device as though it were a local device. It's a useful protocol, so you should turn it on if your NAS device supports it. Find the WebDAV option and enable it. There will be two options: standard and HTTPS (secure). The second option uses an encrypted connection for extra security. Note down the port numbers used by both connections.



STEP 03 Look out for special remote access features, such as the built-in remote access on Western Digital NAS devices. This feature lets you access your NAS from anywhere in the world via a web browser or mobile app (Android and iOS). First, enable remote access to create a username and password, then you can access your NAS remotely at www.wd2go.com or via your mobile app. Some other NAS devices have similar services.



Add or Modify a Virtual Server Entry

Service Port: 21 (XX-XX or XX)

Internal Port: 21 (XX, Only valid for single Service Port or leave it blank)

IP Address: 192.168.0.150

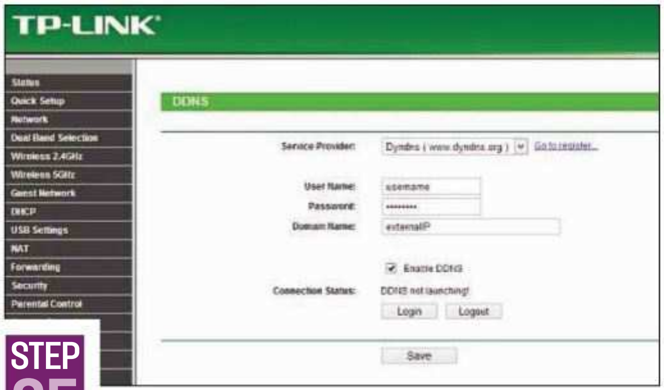
Protocol: TCP

Status: Enabled

Common Service Port: FTP

STEP 04 Connect to your router's web management tool and find the port-forwarding option (also known as 'virtual servers'). Click the Add button to add a new rule. If your router comes with services built in, select FTP from a drop-down list. If not, you'll need to create a new service. Enter a name for the service (such as WebDAV), the start and end ports (the port numbers in Steps 1 and 2) and the traffic protocol to accept (TCP for our services). Tell your router where to send the traffic by entering your NAS device's fixed IP address.

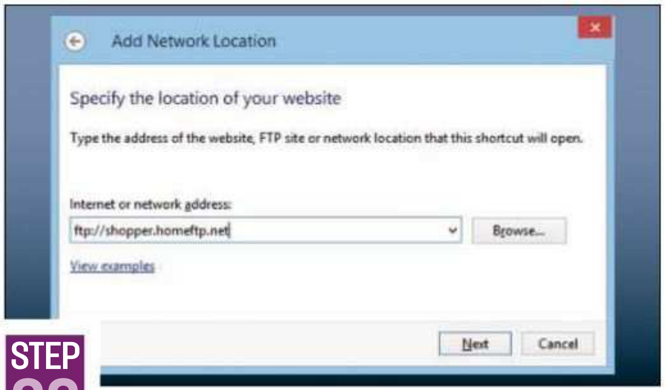
A NAS device is a great way to share files in your home and provide always-on storage. If you're just using your device inside your home, though, you're missing out. Part of the point of having a NAS device that's always on is that you can access it from wherever you have an internet connection. There are several ways you can get access, so in this walkthrough we'll show you all the best options. We're using a Synology NAS device for the purposes of this walkthrough, but the steps are similar for all other NAS devices.



Service Provider: Dyndns (www.dyndns.org)
User Name: username
Password: ••••••••
Domain Name: externalIP
☑ Enable DDNS
Connection Status: DDNS not launching!

STEP 05

Dynamic DNS assigns a web address to your home network. Look for the Dynamic DNS section in your router's management page and pick the service from the drop-down list. We recommend www.dyndns.org, as it's free and easy to configure. Create a new hostname. You can enter anything you want for the first part, but you'll be limited to the domains listed in the drop-down menu, such as homeftp.net. Then go back to your router and type in your username password and complete domain name. You can now access your network by typing in your domain name.



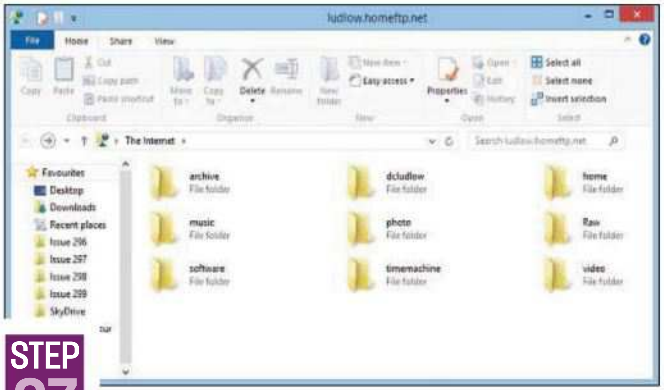
Specify the location of your website

Type the address of the website, FTP site or network location that this shortcut will open.

Internet or network address: ftp://shopper.homeftp.net

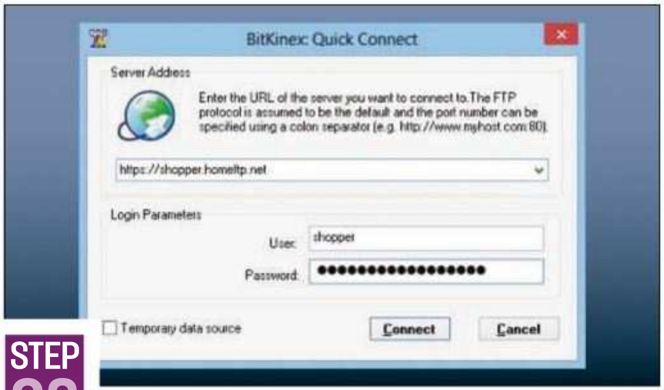
STEP 06

The built-in Windows tool lets you create a permanent icon for a remote connection (FTP or WebDAV) in Windows Explorer. However, Windows' support for WebDAV is poor, but it works perfectly on OS X and Linux, and there are better clients available for Windows. For FTP, start Windows Explorer and select Map network drive. Click 'Connect to a website you can use to store your documents and pictures'. Click Next twice and enter ftp://<your dynamic dns address>. Untick 'Log on anonymously', and enter your username and a name for your connection.



STEP 07

An Explorer window will open, and you'll be prompted for your password. Enter this and choose the option to save your password if you don't want to enter it every time you connect to your server. You'll see that your NAS device is available under Computer as a permanent link that you can use every time you want to access your home storage.



Enter the URL of the server you want to connect to.The FTP protocol is assumed to be the default and the port number can be specified using a colon separator (e.g. http://www.myhost.com:80)

https://shopper.homeftp.net
User: shopper
Password: ●●●●●●●●●●●●●●●●●
☐ Temporary data source

STEP 08

Alternatively, you can use a dedicated application to connect to your server. We recommend FileZilla (filezilla-project.org) for FTP, which lets you resume your transfers. For WebDAV on Windows, BitKinex (www.bitkinex.com) is the best. To configure it, click Connect and type in the address of the server. For WebDav, this is http://<dynamic dns url>:<port number> for normal connections, or https://<dynamic dns url>:<port number> for secure connections. Enter your username and password and click Connect. Your server will be saved to the shortcuts list. ■

CHAPTER 5

5

STREAMING MEDIA

Once you've got your network up and running, one of the most amazing things you can do with it is to stream your photos, videos and music around your home. We'll show you can do this using your PC, TV and additional streaming media and streaming music players. We'll also show you how you can use your smartphone or tablet to orchestrate everything, giving you a powerful multiroom entertainment system for very little money.

CONTENTS

Network components

Your home network will consist of a wide range of products. The illustration on the right shows you an example configuration, but you can add and remove components as you see fit. Here we'll consider the key devices and concepts you need to consider when setting up a home network.

NAS DEVICE

As we explained in the previous chapter, the beauty of NAS devices is that you can leave them on all the time as they draw far less power than a PC, so all the files on the disk can be accessed from any other computer on the network. Most NAS devices have media streamer servers built in. Remote access is usually possible, too, so you can access your files from anywhere with an internet connection.

The cheapest devices have only a single disk, but more expensive models come with two, so you can give your data extra protection. This blend of features makes a NAS device an incredibly useful purchase for most users.

MEDIA STREAMER

If you want to view your digital photos, listen to MP3s or watch your video files from anywhere in your home, you'll need a media streamer. A lot of new TVs will have one built in, but you can buy separate products that connect to any TV.

For music, a dedicated player makes sense. A wireless device is a good choice; you can then carry your player anywhere within range of your network, such as the garden, and still listen to your music library.

PRINTERS

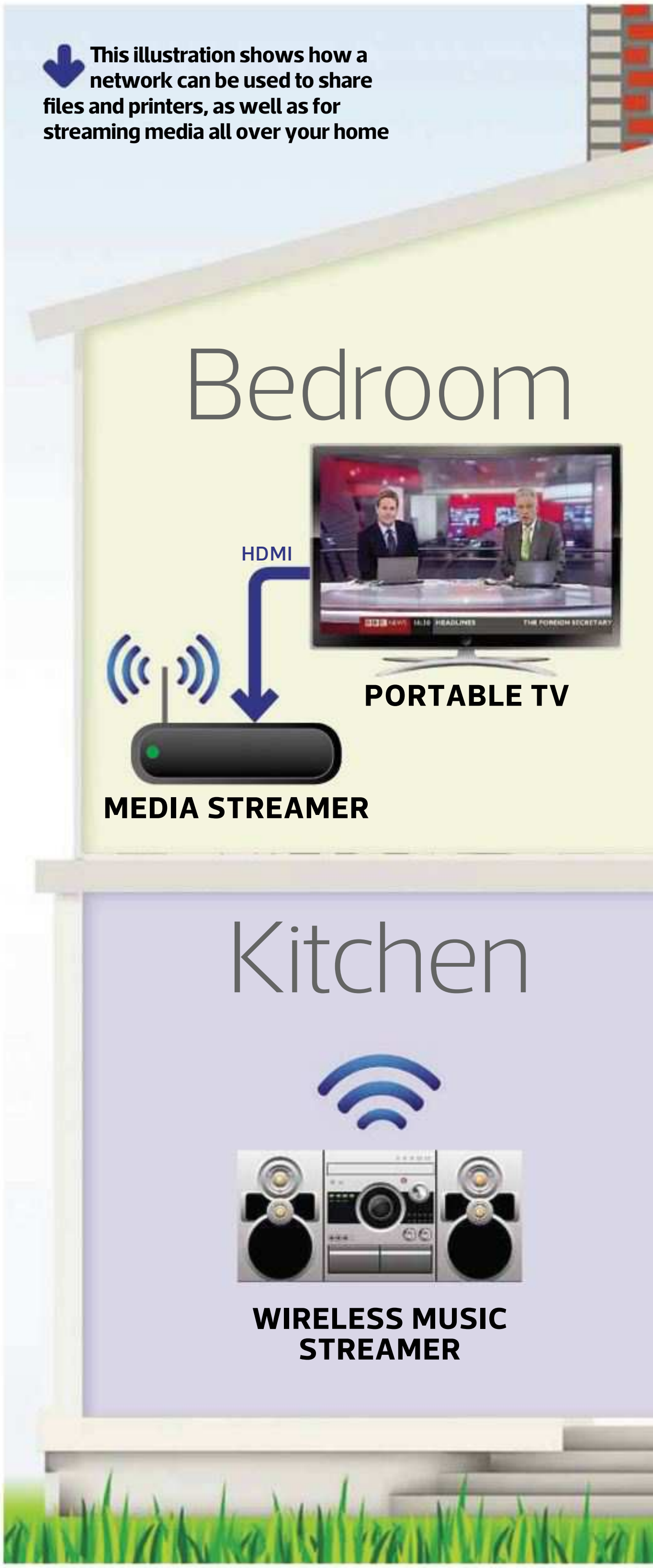
There's no need to buy multiple printers when you can share one over your network. Some attach to your network (either by wired or wireless connections), but even USB models can be shared when connected to a NAS device *(see page 40)*.

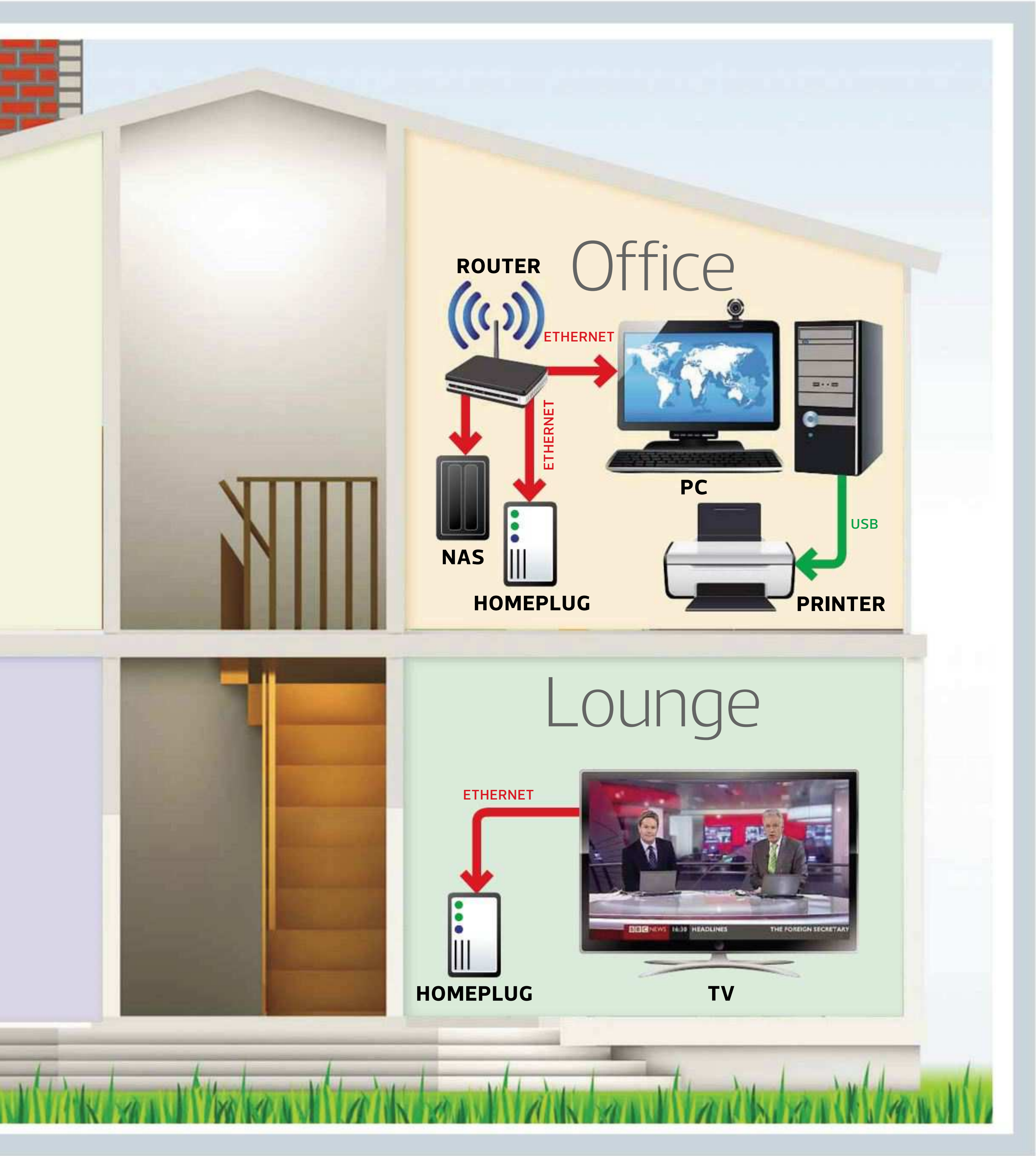
FILE SHARING

A NAS device lets you share your files over a network, but you can also share them directly from your computer. You can do this with Windows, Mac and Linux machines *(see page 33)*.

IDEAL USE OF A NETWORK

This illustration shows how a network can be used to share files and printers, as well as for streaming media all over your home




Office
ROUTER
ETHERNET
ETHERNET
PC
NAS
HOMEPLUG
USB
PRINTER
Lounge
ETHERNET
HOMEPLUG
TV

Sonos gives you multiroom audio, streaming music over your network, although it uses a proprietary networking technology

Media streaming

Media streaming is the technology that lets you send photos, videos and music over your network, letting you play them on other computers and devices. We're going to tell you everything you need to know about playing, managing and sharing your media in the next few pages. Before we start, though, we'll walk you through all the technologies and information you need to know about before you get started.

STANDARDS

There are many different ways of sharing media over your network, depending on the kit you buy. For example, the Sonos multiroom audio system uses its own proprietary network and control system to help you get the most out of it. However, for the vast majority of people, home media sharing is all about Digital Living Network Alliance (DLNA).

DLNA is a technology that uses a protocol called Universal Plug-and-Play (UPnP). All these acronyms basically allow network devices to discover media servers and play the content from them. DLNA is built into a surprising number of devices, from brand-new TVs to the Sony PlayStation 3.

Roughly speaking, DLNA devices can be split into three categories, depending on their abilities. DLNA servers can share their media with other devices, broadcasting what they have available; DLNA players can play content from servers; and DLNA renderers can play content beamed to them from other devices, such as a phone commanding them to pay a certain video file.

Typically, a device will be a combination of the above. For example, a DLNA renderer will also be a basic player, while many servers can also play video files. Unfortunately, it's not always easy to find out what's supported. A lot of networked devices, such as media players, TVs and Blu-ray players, may be marked as supporting DLNA, but generally speaking most of them aren't renderers.

FORMATS

Regardless of the type of player (renderer or straight player), DLNA devices can only play supported video types. So, buy a wireless music streamer, for example, and it will only be able

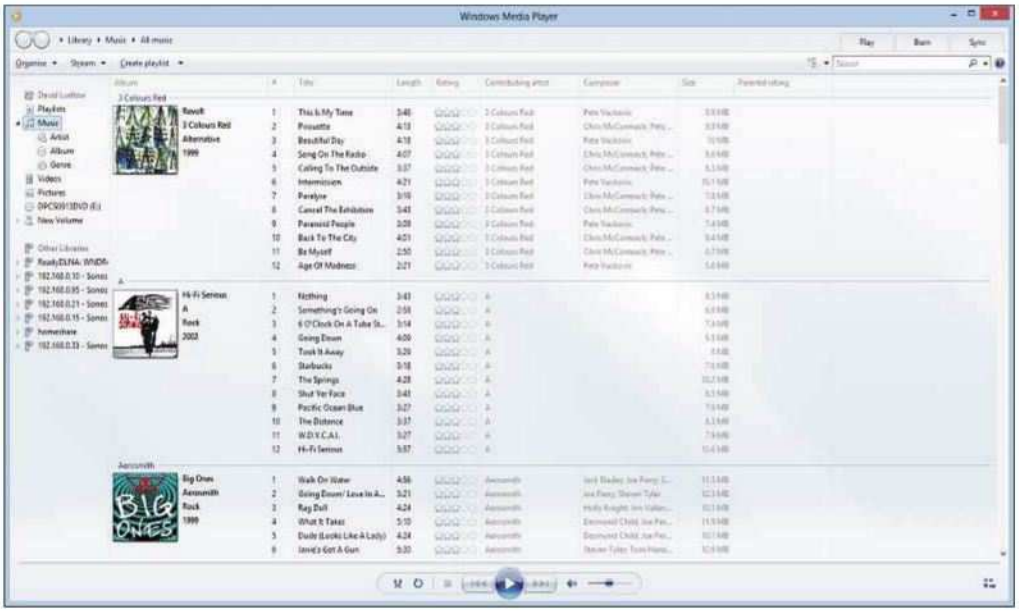
> “DLNA is built into a surprising number of devices, from brand-new TVs to the Sony PlayStation 3.”

As well as being a games console, the PS3 can stream music, videos and photos from DLNA servers

to play audio files and, even then, it can play only the formats it supports. With audio this isn't usually too much of a problem, as audio streamers tend to support the most popular audio formats, such as MP3 and Apple's AAC. Pictures are similarly just as easy to deal with, as most players support all the common file types, including JPEG, PNG and TIF.

However, video becomes more of a problem, as there are a wide range of confusing video format standards, such as MPEG2 and H.264, not to mention DivX and MKV. To make matters more confusing, there are different 'container' files, so a video file with a .AVI extension could actually be an MPEG2 file or H.264 file.

Most media players will happily play most video files, but you may find some formats that won't play. This is particularly true if you want to use Apple's video streaming technology, which has extremely limited support. We'll look at streaming on Apple devices in more detail in Chapter 6, and show you to convert your video files into supported formats on page 62.



David Ludlow
Playlists
Music
Artist
Album
Genre
Videos
Pictures
DPCS0913DVD (E:)
New Volume

Other Libraries
ReadyDLNA: WNDR...
192.168.0.10 - Sonos
192.168.0.95 - Sonos
192.168.0.21 - Sonos
192.168.0.15 - Sonos
homeshare
192.168.0.33 - Sonos

Album	#	Title	Length	Rating	Contributing artist	Composer	Size	Parental rating
3 Colours Red								
Revolt	1	This Is My Time	3:40	☆☆☆☆☆	3 Colours Red	Pete Vuckovic	8.9 MB	
3 Colours Red	2	Pirouette	4:13	☆☆☆☆☆	3 Colours Red	Chris McCormack, Pete ...	9.9 MB	
Alternative	3	Beautiful Day	4:18	☆☆☆☆☆	3 Colours Red	Pete Vuckovic	10 MB	
1999	4	Song On The Radio	4:07	☆☆☆☆☆	3 Colours Red	Chris McCormack, Pete ...	9.6 MB	
	5	Calling To The Outside	3:37	☆☆☆☆☆	3 Colours Red	Chris McCormack, Pete ...	8.5 MB	
	6	Intermission	4:21	☆☆☆☆☆	3 Colours Red	Pete Vuckovic	10.1 MB	
	7	Paralyse	3:10	☆☆☆☆☆	3 Colours Red	Chris McCormack, Pete ...	7.8 MB	
	8	Cancel The Exhibition	3:43	☆☆☆☆☆	3 Colours Red	Chris McCormack, Pete ...	8.7 MB	
	9	Paranoid People	3:08	☆☆☆☆☆	3 Colours Red	Pete Vuckovic	7.4 MB	
	10	Back To The City	4:01	☆☆☆☆☆	3 Colours Red	Chris McCormack, Pete ...	9.4 MB	
	11	Be Myself	2:50	☆☆☆☆☆	3 Colours Red	Chris McCormack, Pete ...	6.7 MB	
	12	Age Of Madness	2:21	☆☆☆☆☆	3 Colours Red	Pete Vuckovic	5.6 MB	
A								
Hi-Fi Serious	1	Nothing	3:43	☆☆☆☆☆	A		8.5 MB	
A	2	Something's Going On	2:58	☆☆☆☆☆	A		6.9 MB	
Rock	3	6 O'Clock On A Tube St...	3:14	☆☆☆☆☆	A		7.6 MB	
2002	4	Going Down	4:09	☆☆☆☆☆	A		9.5 MB	
	5	Took It Away	3:29	☆☆☆☆☆	A		8 MB	
	6	Starbucks	3:18	☆☆☆☆☆	A		7.6 MB	
	7	The Springs	4:28	☆☆☆☆☆	A		10.2 MB	
	8	Shut Yer Face	3:41	☆☆☆☆☆	A		8.5 MB	
	9	Pacific Ocean Blue	3:27	☆☆☆☆☆	A		7.9 MB	
	10	The Distance	3:37	☆☆☆☆☆	A		8.3 MB	
	11	W.D.Y.C.A.L.	3:27	☆☆☆☆☆	A		7.9 MB	
	12	Hi-Fi Serious	5:57	☆☆☆☆☆	A		13.4 MB	
Aerosmith								
Big Ones	1	Walk On Water	4:56	☆☆☆☆☆	Aerosmith	Jack Blades; Joe Perry; T...	11.3 MB	
Aerosmith	2	Going Down/ Love In A...	5:21	☆☆☆☆☆	Aerosmith	Joe Perry; Steven Tyler	12.3 MB	
Rock	3	Rag Doll	4:24	☆☆☆☆☆	Aerosmith	Holly Knight; Jim Vallan...	10.1 MB	
1999	4	What It Takes	5:10	☆☆☆☆☆	Aerosmith	Desmond Child; Joe Per...	11.9 MB	
	5	Dude (Looks Like A Lady)	4:24	☆☆☆☆☆	Aerosmith	Desmond Child; Joe Per...	10.1 MB	
	6	Janie's Got A Gun	5:30	☆☆☆☆☆	Aerosmith	Steven Tyler; Tom Hami...	12.9 MB	

SERVERS

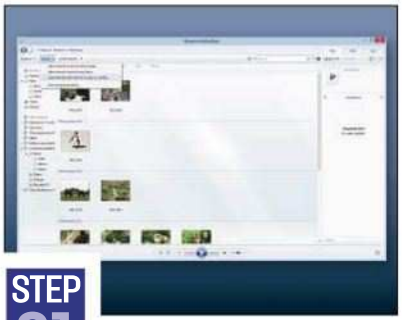
Any decent home network should have a media server for sharing files. A Windows PC will do the job without any new software, but you need to leave the computer on to access its files. A better choice is to use a NAS device, which can be left on all the time.

Over the next few pages we'll show you how to get started with a server on a PC, Mac or NAS device.

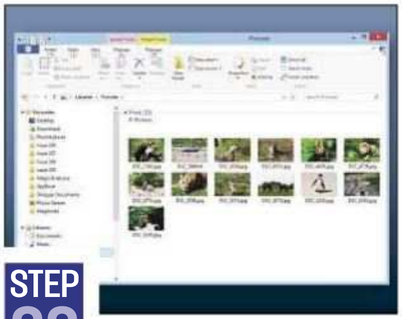
Windows Media Player is a DLNA server, renderer and player

Setting up a media server

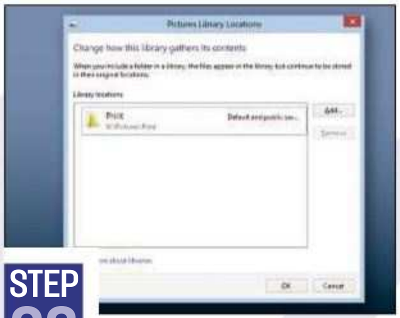
WINDOWS



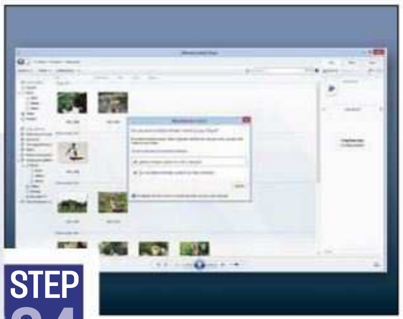
STEP 01 Start Windows Media Player from your computer and it will load, letting you play all your media files. At this point it's not configured to share anything, so you need to turn on media sharing. At the top of the screen click Stream, then select Automatically allow devices to play my media. On the next screen click 'Automatically allow all computers and media devices' to turn on media sharing.



STEP 02 Windows Media Player will now share all your media files, but you need to make sure they're stored in the correct folder. Media Player uses Windows Libraries and, by default, looks in the Music, Videos and Pictures Libraries for your files. You can access these by opening a Windows Explorer Window and selecting the relevant Library under Libraries, in the left-hand panel. Make sure your media files are stored here.

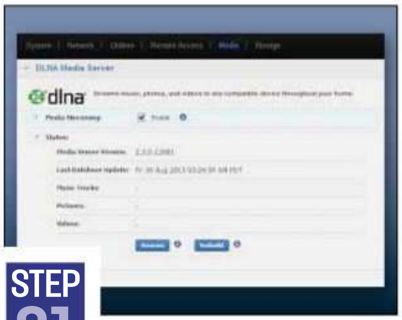


STEP 03 If you'd rather keep files in different folders, you can change where Libraries look for files. In Media Player, right-click Music, Video or Pictures and select 'Manage <name> library'. In the next screen you'll see a list of folders. Click Remove if you don't want to use a folder any more. To add a folder, click Add, browse to it and click Include Folder. Click OK when you're done and repeat for any other Library you want to change.

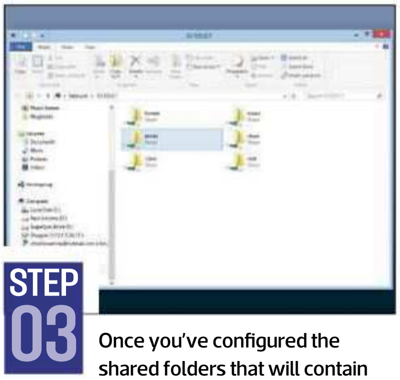


STEP 04 With all your files in the right folders, Windows Media Player is now sharing your folders, provided that the software is running and your PC is turned on. Before you move on to trying to play media, if you want to be able to send files to your PC, click Stream, Allow remote control of my player. On the next screen, click 'Allow remote control on this network'.

NAS

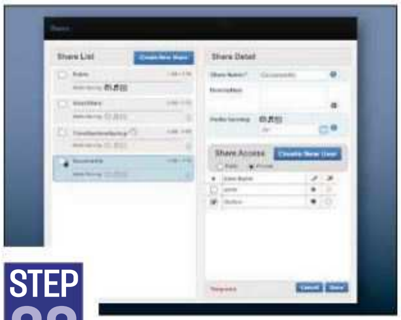


STEP 01 Connect to your NAS device's web-based management page following the instructions in Chapter 4. The steps differ for each manufacturer, although they're roughly the same for all devices, so check your manual for the exact steps. Look for the media server option and turn it on.

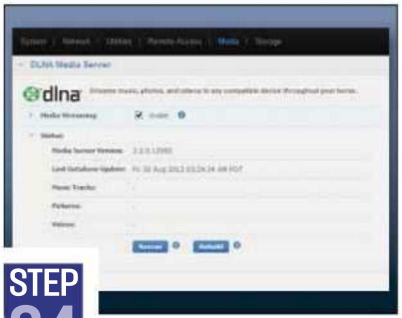


STEP 03 Once you've configured the shared folders that will contain your media, copy the files over the network to the server. Depending on the size of your media collection, this may take a while to complete.

A media server lets you share you music, photos and videos with your entire network. Configuring a media server is really easy. If you have a PC or a NAS, the chances are that you have the technology you need built in. With Mac OS X it's a little harder, as it supports only Apple's streaming out of the box; however, there are free add-ons available you can use. Here we'll show you how to get a media server up and running, no matter what you're using. In our opinion, using a NAS is the best option, as it's always on, but the other methods will still do the job.

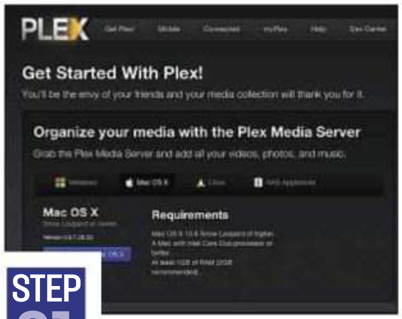


STEP 02 You'll need to configure which shared folders are set up for media sharing. Some NAS devices create dedicated folders for photos, videos and music; other NAS devices let you choose which folders are for media sharing. Check your device's configuration to see which type you have and turn media sharing on for some folders.

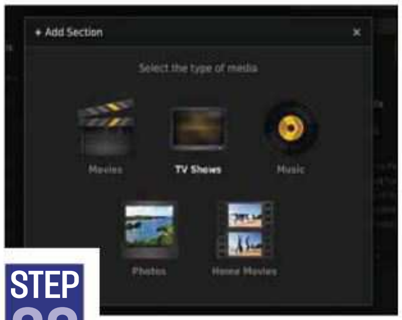


STEP 04 Your media files should be ready for playing immediately, but some times it can take a while for your NAS to index them. In this case look for the option to Rescan, which will detect new files. If you're having real problems, a Rebuild option will force your NAS to rebuild its media index from scratch.

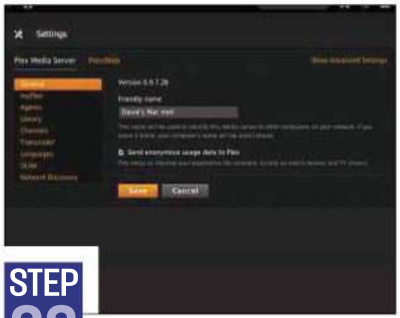
MAC OS X


PLEX
Get Started With Plex!
You'll be the envy of your friends and your media collection will thank you for it.
Organize your media with the Plex Media Server
Grab the Plex Media Server and add all your videos, photos, and music.
Mac OS X
Requirements

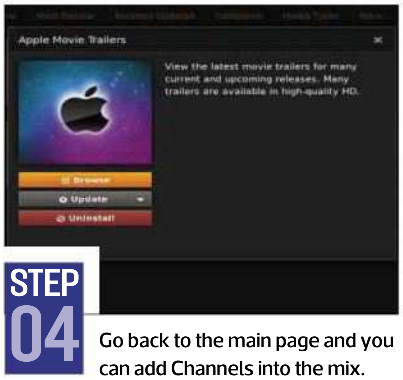
STEP 01 Mac OS X doesn't have a UPnP server built-in, so you need to download an alternative. We recommend the excellent Plex (www.plexapp.com), which is also available for Windows. Go to the website and click Get Plex!, click Mac OS X and click Download for Mac OS X. When the file has downloaded, run it and copy the app to your Applications folder. Run the media server once you've done this.



STEP 02 The first time you start Plex, you'll be taken to a web page that lets you configure the software. The first thing to do is to add media to your server. Click the '+' icon under My Library, then select a type of media. Next, click Add folders and browse to where your files are stored and click Add. In OS X the default media folders are stored in Users/<your username>. Once done, you'll be taken to a web page dedicated to the new section.



STEP 03 Back on the main page you can click the settings icon – a spanner – to change how the server works. You shouldn't need to change much here, but you might want to change the name of your server, so it's easy to distinguish it from other devices. You may also want to disable 'Send anonymous usage data to Plex'. Click Save when you're done.


Apple Movie Trailers
View the latest movie trailers for many current and upcoming releases. Many trailers are available in high-quality HD.
Browse
Update
Uninstall

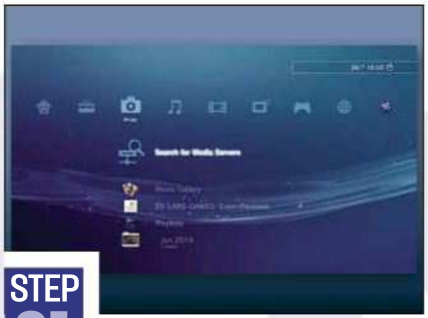
STEP 04 Go back to the main page and you can add Channels into the mix. Click the '+' icon under Channels and you'll see a list of optional online services, such as Apple Movie Trailers and TED. Installing these will let your media players access these services, too. Click on the ones you want to use and click Install for all the services you want.

Streaming media

Once you've got your media server up and running on your network and you've loaded it up with all your files, you need a method of playing the content. This is where a media player comes in. A media player can be anything from a TV with a built-in DLNA client – which a lot of modern Smart TVs have these days – or a dedicated media player.

Players can be audio-only or multimedia, which means they'll also play video files. Typically, audio players have their own individual setup routines and are controlled through a dedicated smartphone app, so this guide focuses on how to use a multimedia streamer; however, the instructions may be useful for when you first set up your audio player. We're using a Sony PlayStation 3, but the instructions and prompts are roughly similar for all devices.

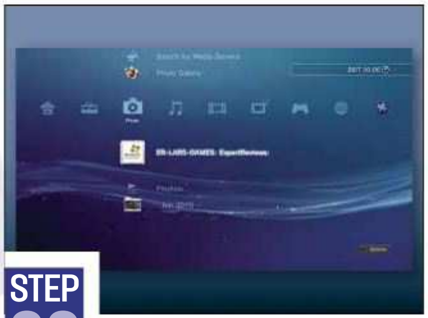
Before you begin, make sure your media server is turned on and running, and that your media player is on and connected to the same physical network.



STEP 01

FIND SERVERS

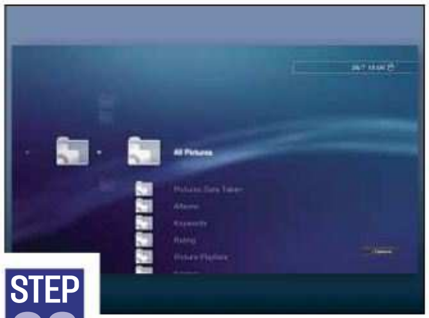
Some media players will automatically find media servers on your network and connect to them, but some will require you to search for them first. If your player has this option it will scour the network looking for any media players. This can take a few minutes to complete. You media player should then list your media server.



STEP 02

CONNECT TO SERVER

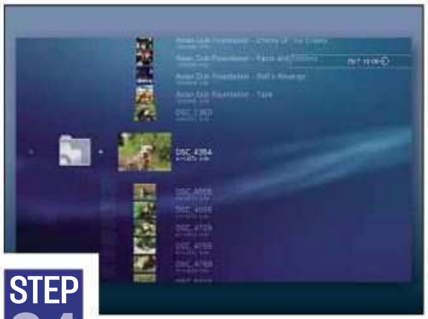
Most media players split media into three categories: photos, videos and music. Each one defines the type of media the player will find. We'll start with photos; select the photos category of your player, then select your server; alternatively, you may need to select your server first, then select photos.



STEP 03

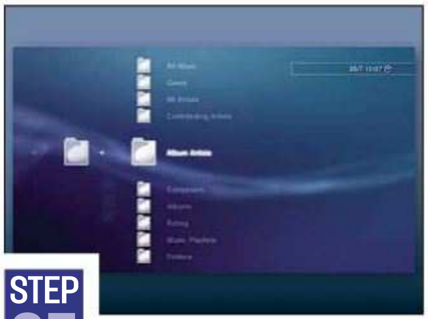
VIEW PHOTOS

When you're looking for photos you'll most likely find you get a list of folders you didn't create, such as All Pictures, Pictures Date Taken and so on. These are created by the media server, automatically categorising your photos, so you can view them in any order. However, you can also select folders to browse through your photos in the same order in which you stored them originally.



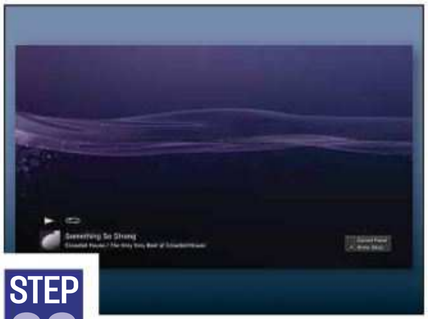
STEP 04 SLIDESHOWS

Once you've chosen your folder, you can browse through the list of thumbnail pictures and select the one that you want. Look out for an option to start a slideshow. You can usually also skip between photos by using the direction pad or chapter skip buttons on a remote control. Be careful, as photos can be quite large, so they can take a while to appear on a TV.



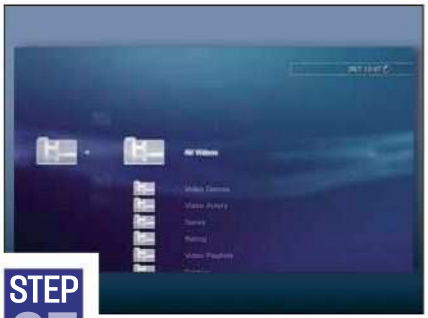
STEP 05 LISTEN TO MUSIC

Follow Step 2, but this time choose the music option. Just as with photos, you'll find you get the option to choose music by a variety of different methods, such as genre, artist and album. This information is pulled from the music track by the media server automatically, much in the same way as an iPod does. Browse through your music until you find the album or track you want to listen to.



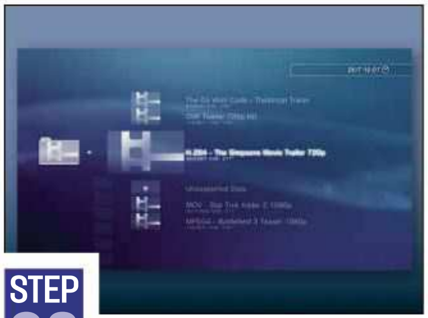
STEP 06 PLAYLISTS AND MORE

Once you've selected a track it will start playing. You can use the normal playback controls to pause and fast-forward or rewind, while track skip controls will move to the next or previous track. Look for advanced options to create playlists, although not all media players support this feature. Typically, while music is playing you can go back to photos and browse through your picture collection.



STEP 07 WATCH A VIDEO

Follow Step 2, but this time select videos. Again, you'll see a list of folders that you didn't create, such as Video Genres and Video Actors. This is created by your media server using information built into the video files. However, we find this an unreliable method, as the information is often missing. It's usually easiest to select folders and simply browse through your files.



STEP 08 CHOOSING A FILE

Video files will sometimes have a thumbnail preview, but this is by no means universal. Here, more than with any other file type, you'll find some files that won't play or are listed as unsupported. That means your media player doesn't support the video's file format. You'll need to convert the files to a different format using the instructions on page 60.

STEP 09 PLAY A FILE

Select a file to play it. You can use the normal playback controls, just as you would when watching a DVD. However, the chapter skip buttons will work properly only if your video file has embedded tracks; many don't, so this feature often isn't very useful.

Converting videos for free

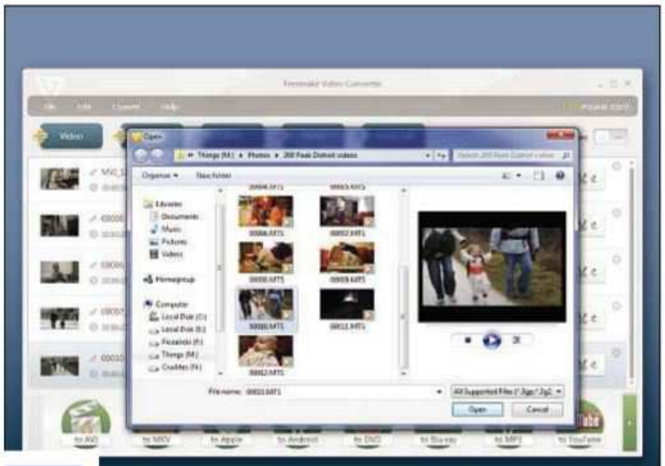
Converting videos to play on a portable player can be a minefield. We reveal a free utility that makes high-quality conversion simple.

Today's computers are bursting with videos but a PC monitor isn't always the best place to view them. Transferring videos to a mobile device – be it a phone, MP3 player or tablet PC – means you can watch them while travelling and share them with friends and family.

The downside is that many portable players are extremely fussy about which types of file they can play. It's hardly surprising, given that a video file has around a dozen encoding parameters. Even for the more flexible players, it's important to use settings that deliver high quality in efficient file sizes. Videos are big files, and choosing the wrong format can waste gigabytes of valuable space on your player.

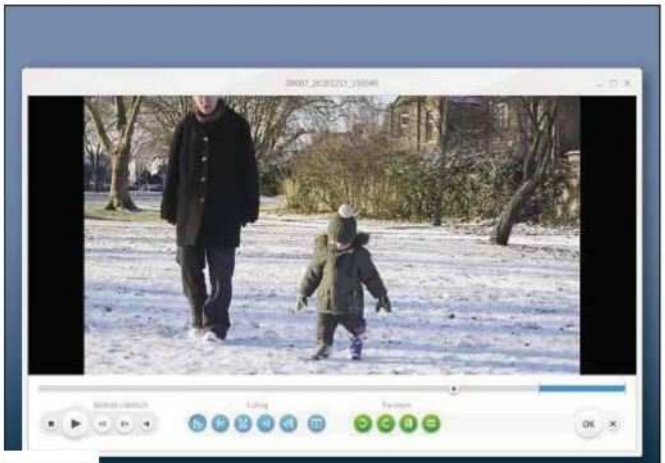
We've tried lots of video-conversion utilities, and one of the best tools happens to be free. Freemake Video Converter can import and export a massive range of video formats, and converting is usually a simple matter of choosing the template for your player. Best of all, it chooses export settings that are not just compatible with the player but are also sympathetic to the source material. Unlike many conversion utilities we've seen, it won't arbitrarily change the frame rate, and while it happily reduces the resolution to match your player's screen resolution, it won't needlessly boost the resolution of smaller source videos.

Download the Freemake Video Converter utility from www.freemake.com and install it before following the steps on the right.



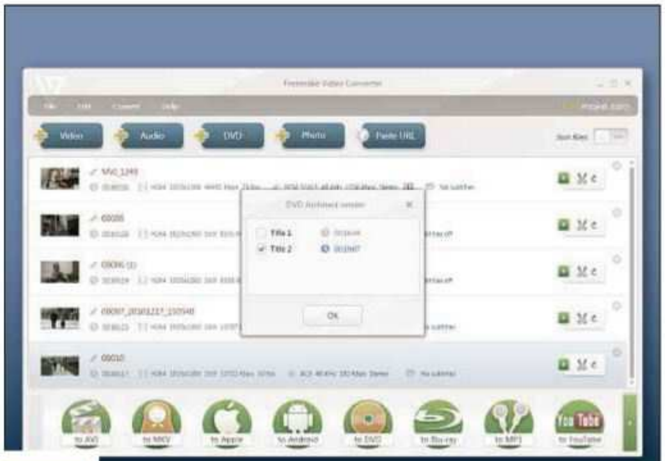
STEP 01

Importing videos couldn't be simpler: just drag and drop files from Windows Explorer on to the central window in Freemake Video Converter, or drop a folder to import its entire contents. Alternatively, you can drop a file or folder on to the software's desktop link and it will launch automatically with the files ready to convert. If you prefer to do things the old-fashioned way, click the +Video button at the top of the screen and browse to the files you want in the dialog box that appears. Hold down the Ctrl key to select multiple files, or hold Shift and click the first and last files to select a sequence.



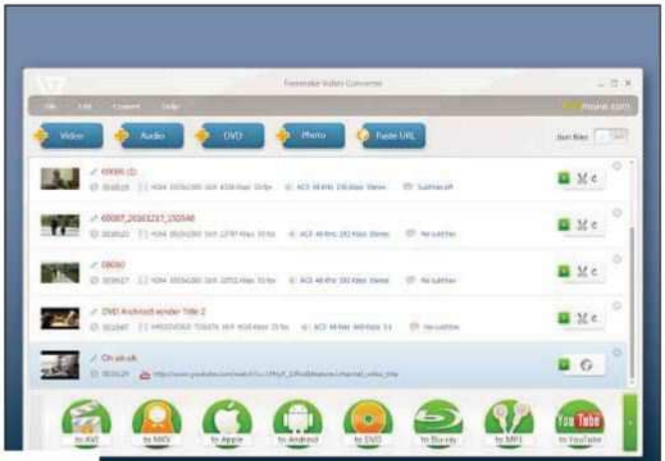
STEP 04

Each entry in the imported list includes various information, plus options to change to a video's alternative soundtrack and to include subtitles, if available. The edit button to the right of each video reveals controls to trim out unwanted sections. Use the transport controls to identify a cut point, and use the buttons in the Cutting section to define the Start Selection and End Selection points. Click Cut Selection to remove that section. Click OK to return to the main window. Consider whether you want to enable the Join files option at the top-right of the screen, which strings all the imported media together into a single exported file.



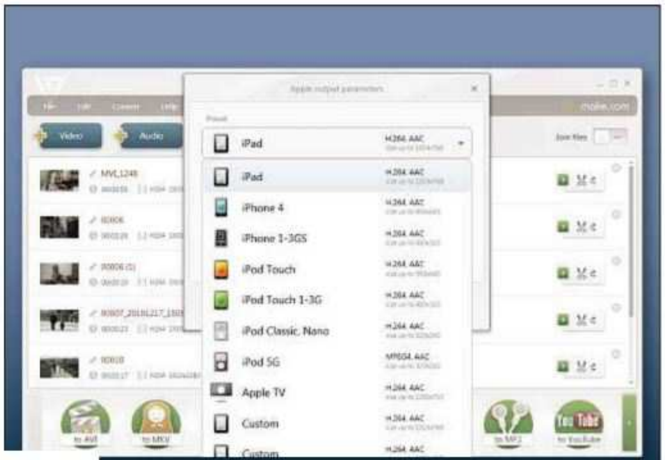
STEP 02

The software isn't limited to converting videos. Import a collection of photos, for example, and it will turn them into a video slideshow. Audio files can be converted to a suitable format for your media player, too. Import a folder of DVD files and it will present a list of the disc's contents, allowing you to choose just the main feature and omit any extras (although it won't circumvent the CSS encryption used on commercial discs).



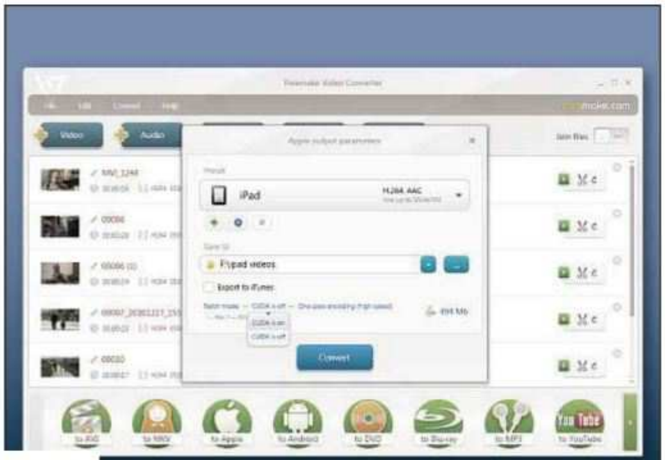
STEP 03

It's even possible to import videos directly from YouTube, Facebook, Vimeo and many other online video-hosting sites. Simply navigate to the video you want to import in your web browser, select the page's URL in the address bar and type Ctrl-C to copy it. Back in Freemake Video Converter, click Paste URL and the video should appear in the imported media list. When you come to convert it, the software will download the video at the highest available quality before converting it to your desired settings.



STEP 05

Now it's time to export your videos. Most portable players have export templates ready and waiting, arranged in various categories across the bottom of the screen. Choose Apple, for example, and you'll see a list of presets including iPad and various generations of iPhone and iPod. Android presets are sorted by screen resolution; a quick Google search will confirm your phone or tablet's screen resolution. Use the scroll button to see further export template groups, such as Sony PSP and 3GP (for older phones). When you've found a suitable template, choose a destination on your hard disk to save to and click Convert.



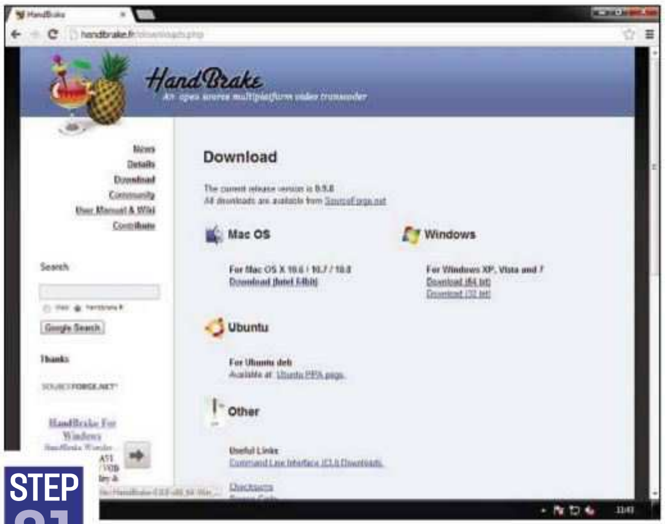
STEP 06

Freemake Video Converter makes sensible choices about bit rates, but if you would prefer a cleaner picture at the expense of bigger files, try increasing the bit rate manually. Import files one at a time, choose a preset as before, but before clicking Convert, increase the predicted export file size by around 50 per cent. Choosing Two-pass encoding can also boost quality a little, but it doubles the encoding time. Other options include CUDA encoding, which uses the processor on an Nvidia graphics card to encode the file, and Export to iTunes, which means your videos will appear in iTunes, ready to transfer to your player.

Converting video files for Apple

Apple's streaming media players require very specific file formats, but converting videos is easy thanks to the free HandBrake app.

It's always best to watch video at the maximum resolution supported by the playback screen, but on a smartphone or tablet this could be smaller than the original. While many devices can scale video on playback, you'll get the best quality and use less storage space if you convert to the right resolution before copying it to the device. On the other hand, you'll have to convert a video if it's in a format that the destination device doesn't support; AirPlay streaming to an Apple TV requires H.264 encoding, for example. Here we'll show you how to do the job easily with HandBrake, a free video transcoder.



Download

The current release version is 0.9.8
All downloads are available from SourceForge.net

Mac OS

For Mac OS X 10.6 / 10.7 / 10.8
Download (Intel 64bit)

Windows

For Windows XP, Vista and 7
Download (64 bit)
Download (32 bit)

Ubuntu

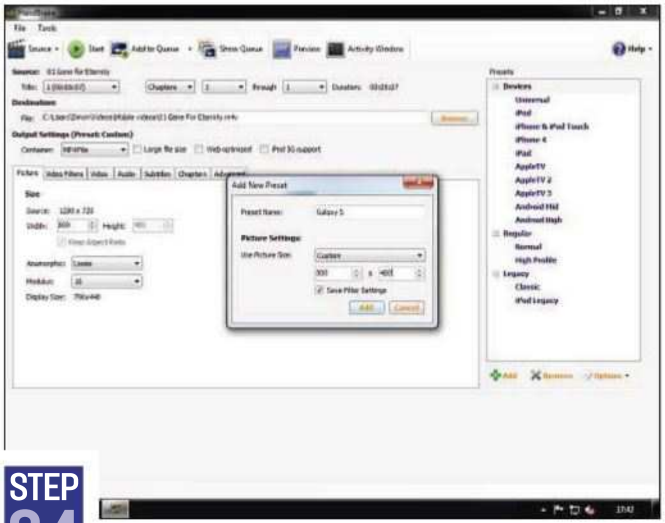
For Ubuntu deb
Available at Ubuntu PPA page.

Other

Useful Links
Command Line Interface (CLI) Downloads
Checksums

STEP 01

Visit handbrake.fr, click Download and choose the relevant installer. Although Windows 8 isn't listed, HandBrake will work perfectly on the latest version of Microsoft's operating system, but for any Windows version be sure to download the correct 32- or 64-bit installer. Run the download, agree to the licence terms, choose an installation location and click Install. Once this has finished, start the application by double-clicking on the desktop icon.



Add New Preset

Preset Name: Galaxy S

Picture Settings:

Use Picture Size: Custom

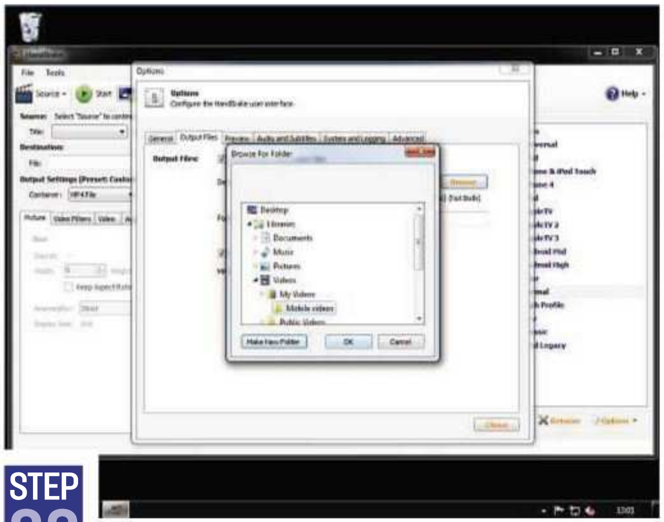
800 x 480

☑ Save Filter Settings

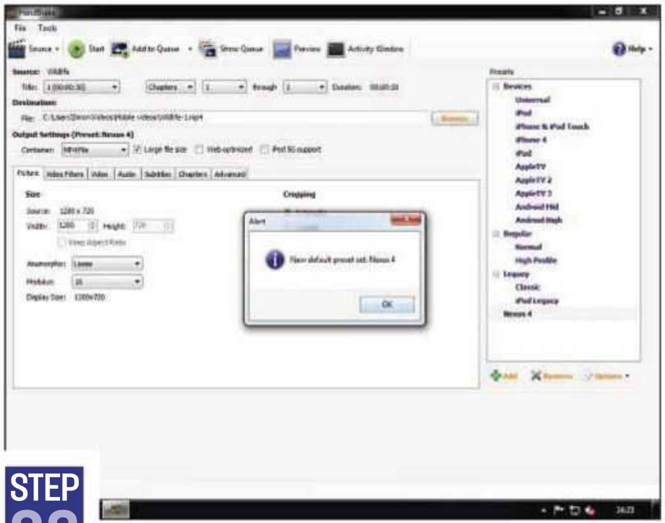
Add Cancel

STEP 04

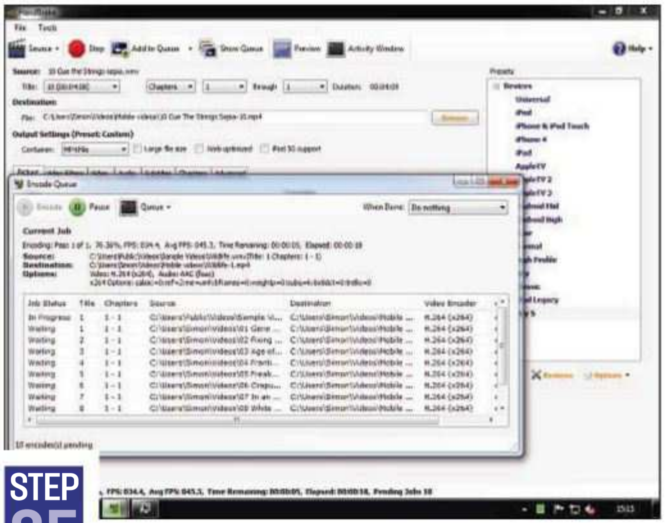
Click Add under the Presets list to create a new preset. Give the new preset a name, select Custom from the Use Picture Size box and enter the screen resolution of the device, which you can usually find on the manufacturer's page or by simply searching the web. Remember that the resolution of a mobile device is usually given with the smaller number first (ie, a portrait orientation). In most cases you'll want to watch videos in landscape orientation, so simply swap the two numbers if necessary. Make sure Safe Filter Settings is ticked then click Add to save the preset, which should appear at the foot of the list.



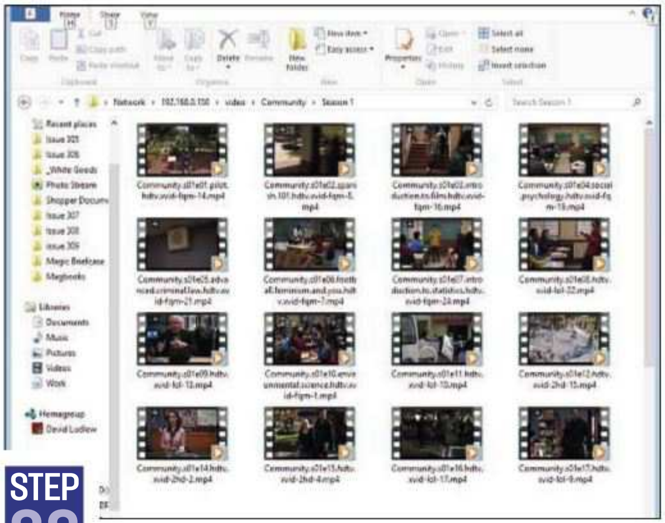
STEP 02 When HandBrake starts, click the Tools menu, select Options and click the Output Files tab to specify a location for your converted video files. In most cases these will be at a lower resolution than the original file, or at least they will have been transcoded from it with a small loss of quality, so we'd recommend that you create a specific folder such as 'iPad videos' so you can store them separately from the originals. Click Browse, navigate to the folder you want and click OK, then click Close to dismiss the Options dialog box. With this done, click the Source button and choose either a video file or folder.



STEP 03 For optimal video quality on your mobile device, it's important to choose the right settings. HandBrake comes with a useful set of presets created for popular devices such as the iPhone or iPad. If yours appears on the list, simply click to select it. If it's your only device you may also want to set it as the default by clicking the Options button beneath the list and choosing Set Default. With this done move, on to Step 5. If your device isn't on the list you can create a new preset, although you may first want to check the settings in the Picture tab as these can be saved with the preset. We'd recommend selecting Loose in the Anamorphic setting box.



STEP 05 Once you're happy with the settings, click Start to begin transcoding a single file or, if you're transcoding a folder, click Add to Queue, then drop down the Title box and move through the folder's other files, checking the settings and enqueuing each. When the queue is full, click Start to begin the transcoding. Remember that it's an intensive process that will work your PC hard, typically causing an increase in cooling fan noise, and that transcoding feature-length content may take several hours. It may be best to perfect the settings on a single file, then enqueue a batch of files to run overnight.

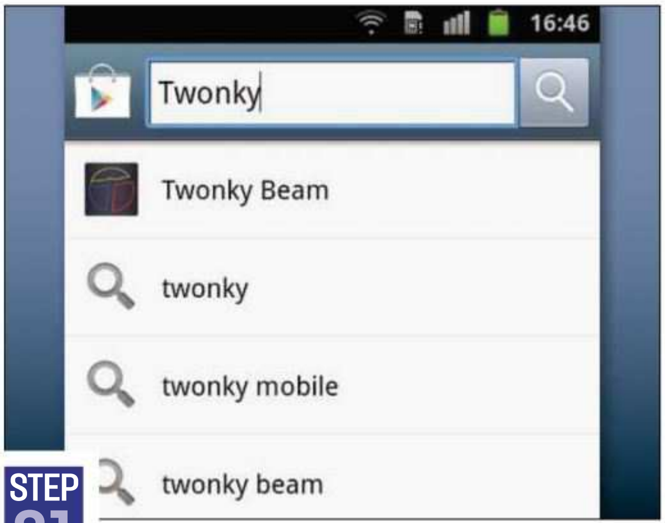


STEP 06 With your files converted to the right format, you can copy them back on to your media server. You may want to delete the original files, so you don't have two copies of each video, but you can always move them somewhere else for backup. You will now be able to play your videos from any Apple device.

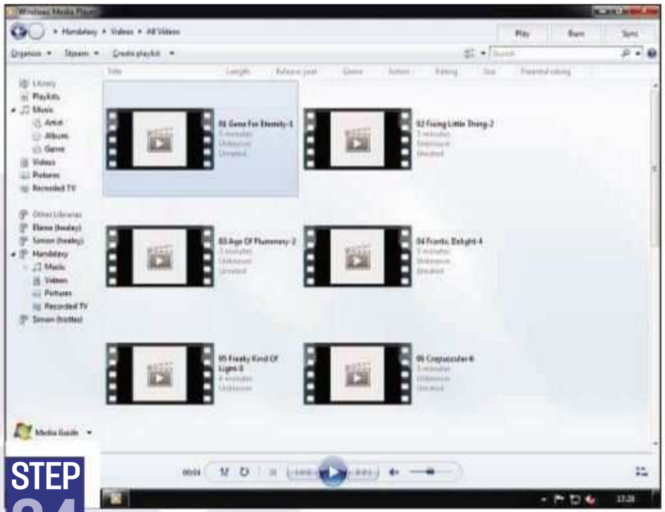
Beaming files from your smartphone

Your smartphone can be used as a smart remote control, beaming audio, video and pictures from your PC to a network player.

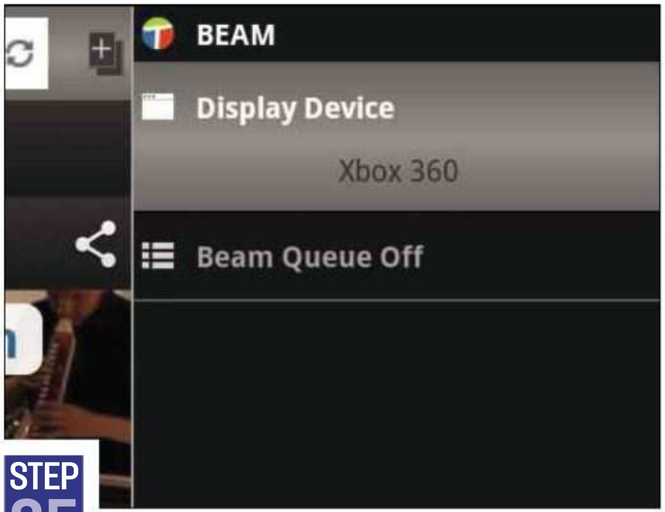
A smartphone is great for watching movies while you're out and about, but it's not so great to be stuck with its small screen when you're at home. You can copy unprotected media to a PC and watch it there, but there are apps that will let you stream almost anything directly from your phone to a computer, or another UPnP device, such as a games console. We'll show you how to use Twonky Beam to bring an iPhone or Android phone into your living room. For this to work you need a DLNA Renderer on your network. If you have one it will appear in the App's beam menu; if you haven't, you'll need to use standard streaming.



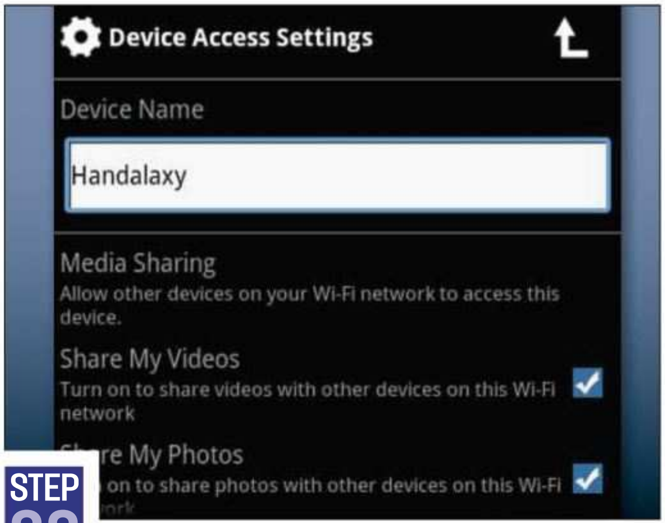
STEP 01 Beaming media will work only where your phone is connected to the same network as a suitable UPnP device, so at home make sure Wi-Fi is enabled on your device. Once joined to the network, open an Android phone's Applications menu and tap Play Store, then tap Apps, search for Twonky and tap Twonky Beam in the results. Tap Install, review the permissions and tap Accept & download. With the app installed, tap Open to run it for the first time, or find it via the Applications menu and tap its icon from there. On an iPhone, search for Twonky in the App Store, select Twonky Beam in the results and tap Free, then Install to install it, providing your Apple ID password if prompted. Click OK at the age-restricted content warning. Tap Twonky Beam to start the app.



STEP 04 As a UPnP server, Twonky Beam should work with any compatible player. In Windows Media Player, for example, switch to the Library view and the server should appear in the list to the left. Double-click to open it and browse its contents as you would any other source, and double-click to play a file. If playback is sketchy, move the phone near the router, or reduce the bandwidth setting described in the previous step.



STEP 05 Twonky Beam can also beam content at a playback device. To choose your Playback device swipe in from the right to bring up the Beam menu. Select your playback device. Use the app's icons to navigate for content on sites like YouTube and, where supported, tap Beam and select a Display Device. Tap Beam again and the device should automatically begin displaying it. Scroll the icons at the base of the app to access the playback and volume controls.



Device Access Settings

Device Name

Handalaxy

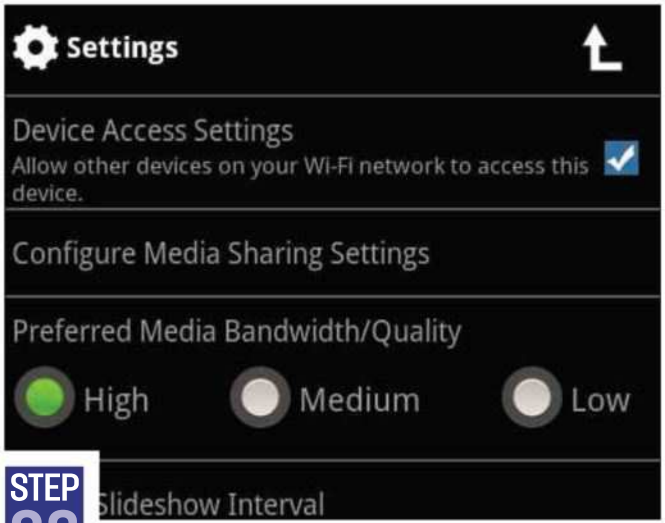
Media Sharing
Allow other devices on your Wi-Fi network to access this device.

Share My Videos ☑
Turn on to share videos with other devices on this Wi-Fi network

Share My Photos ☑
Turn on to share photos with other devices on this Wi-Fi network

STEP 02

Once the app has started, review and agree its terms of service, unticking the 'share information' option if you want before tapping OK. Tap Next and Dismiss to clear the startup tips. Before you beam content, you'll need to visit the Settings menu by tapping the gear wheel icon in the bottom right-hand corner of the screen, then tapping Settings. On the Settings page you'll need to tick the box next to Device Access Settings, then tap Configure Media Sharing Settings. On the next page, give your phone a device name and select which media types you want other devices to access. You can also tell Twonky Beam to remember your settings for your network.



Settings

Device Access Settings ☑
Allow other devices on your Wi-Fi network to access this device.

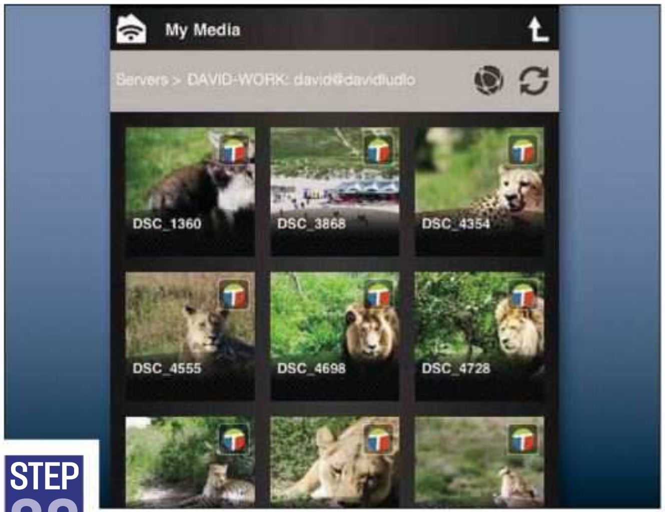
Configure Media Sharing Settings

Preferred Media Bandwidth/Quality
● High ○ Medium ○ Low

Slideshow Interval

STEP 03

Tap back to return to the Settings menu, then choose a bandwidth setting. We recommend trying High initially, but be prepared to return to this menu and try a lower quality if you experience drop-outs or stuttering playback. Tap back twice to return to the app's main screen. Your phone should now be sharing its media content over your network.

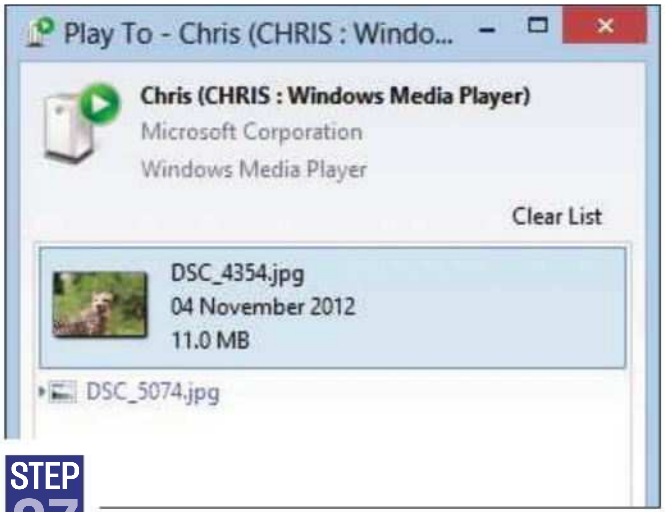


My Media

Servers > DAVID-WORK: david@davidludlo

STEP 06

Twonky Beam can send video from your home network's media server, too. Tap the My Media icon at the top of the home screen (it looks like a house with a wireless signal in it) to bring up a list of all the servers on your home network. Browse to the media you want, then tap it to beam that media to your chosen device. You can also select Beam All to send all media, such as a collection of photos, although you'll get a prompt asking you to turn the Beam Queue on first.



Play To - Chris (CHRIS : Windo...

Chris (CHRIS : Windows Media Player)
Microsoft Corporation
Windows Media Player

Clear List

DSC_4354.jpg
04 November 2012
11.0 MB

DSC_5074.jpg

STEP 07

You can also beam files directly from Windows. Just browse to the folder containing the files you want and select the ones you want to send. Right-click them and select Play to, <device you want to send them to>. You'll see a playback window with the list of files you're sending. You can use the playback controls to pause, play and skip through files, and drag and drop new files to the list. Existing files in the list can be removed by selecting them and hitting the Delete key. ■

MENU
▶ II
tv

6

STREAMING MEDIA WITH APPLE KIT

Apple handles streaming differently to everybody else. In this chapter we'll explain exactly why Apple AirPlay is different, look at how Apple TV can be an essential component of your network and show you how to release your digital content from elsewhere. We'll also show you how to use your iPhone or iPad as a remote control, giving you an amazing home entertainment system.

CONTENTS

Introduction to Apple TV

You don't expect Apple to follow everyone else's lead, and Apple TV certainly doesn't. It's like no other media streamer; in fact, from the interface there is no way to stream content from your home network.

Before you write it off, though, it's important to understand that Apple TV is different for a reason, and it's actually rather good. For starters, the box is tiny and it costs just £99, making it one of the better-value media streamers available. It's also extremely easy to use, as you'd expect from an Apple device.

Apple has focused on bringing you content using iCloud, which means you don't even need to have a server in your house. The iCloud service enables you to access and stream movies and TV shows that you've bought or rented from the iTunes store. You can also buy or rent content from your Apple TV and view it on an iPad or iPhone later.

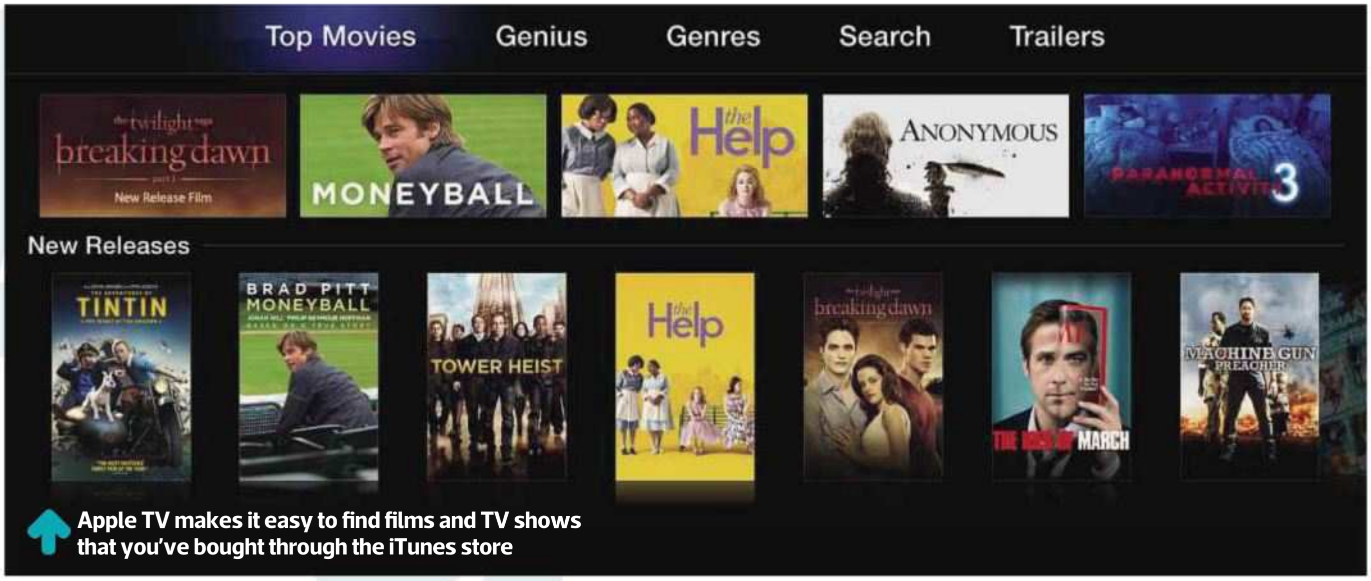
Apple has done a great job of making content easy to find. You can browse films and TV shows by the ones you've bought, top programmes, genres and networks and search for content. It also has Genius built in, which will recommend content based on the shows you've already bought or rented.

In terms of content, there's a lot on offer, with the latest films to buy or watch. TV programmes are similarly up to date, and there are even shows to buy that are currently being shown on TV; the only restriction is that the iTunes version is delayed by at least a day. We like the Series Pass, which lets you buy an entire series before all the episodes have been aired, so each week you get a new episode to watch.

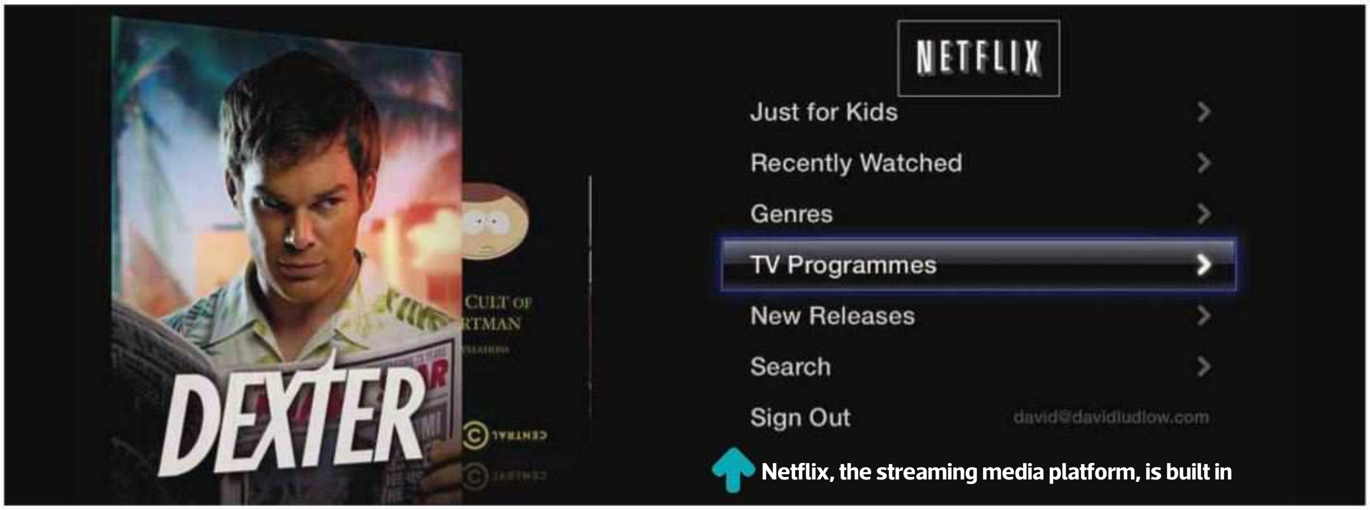
FLIX AND PICS

Not that you have to rely on Apple content, as Netflix is also built in. If you have a monthly subscription, you can stream 1080p movies and TV programmes direct to the Apple TV. Apple has designed its own Netflix interface to match that of Apple TV, which is a great idea, as it keeps the interface consistent across every part of the system.

Photo Stream is also built in, and pulls in all your photos stored in iCloud. It's very smooth, pulling down a set of photos at once, so there's no delay moving between them, making it feel more like you're accessing local storage. There's also a Flickr app you can link to your online account.



Apple TV makes it easy to find films and TV shows that you've bought through the iTunes store



Netflix, the streaming media platform, is built in

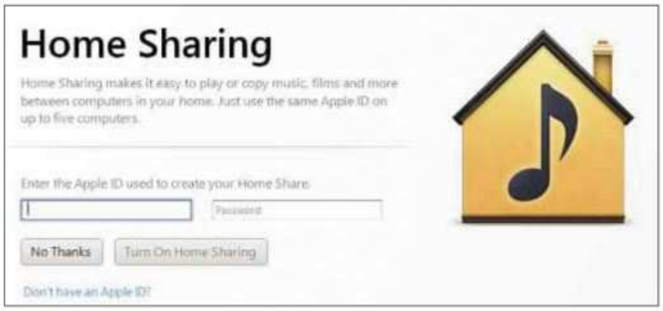
For the Music app you need to turn on iTunes Match, which costs £22 a year. This service determines which songs in your collection are available from Apple, then only uploads the songs in your library that aren't. Once the matching's done, your entire music collection can be streamed using 256Kbit/s AAC files, so you don't need to have a PC turned on to share music. There are also Podcasts and Internet Radio apps built in.

One of the main advantages of a media streamer is its ability to view content that's stored locally on your network. On Apple devices, you can use the Computers app, which pulls in content from computers running iTunes with Home Sharing enabled.

To do this, start iTunes on your computer and select Home Sharing from the drop-down menu under the playback controls. Enter the same Apple ID and password that you used to log in to your Apple TV and select Turn On Home Sharing. All the music, videos and photos you have in your iTunes library will now be accessible from your Apple TV.

THE DRAWBACKS

Unfortunately, Apple TV will not work with any type of media server, such as one running on your network, and will not even work with media servers that have iTunes media sharing (this is different to Home Sharing).



Home Sharing

Home Sharing makes it easy to play or copy music, films and more between computers in your home. Just use the same Apple ID on up to five computers.

Enter the Apple ID used to create your Home Share

You need to turn on Home Sharing if you want to stream music, videos and photos from your iTunes library to a PC

Nor is its file support much cop, with H.264 your only option for video. However, if you've bought all your content through Apple and use iTunes to store your files, then none of this is a problem, and Apple TV works brilliantly.

What's more, the restrictions become less of an issue if you also have an iPad or iPhone, thanks to AirPlay. AirPlay is Apple's way of sending audio and video from one device to another. So if you're watching a video on your iPad, for example, you can send it to Apple TV and watch it on the big screen. There are limitations, however, and you can only play video formats supported by Apple TV over AirPlay. This means that a DivX video playing in an app on the iPad can't be sent to Apple TV, but a QuickTime video can be.

AIRPLAY ADVANTAGES

Using AirPlay becomes really useful when you want to use a UPnP server on your network, such as one included with your NAS. Using your iPad or iPhone you can use a media player app that supports UPnP to stream content from your server, which you can then send to Apple TV via AirPlay. It effectively turns your iPhone or iPad into a giant remote control *(see page 72)*.

One of the beauties of AirPlay is that once you send the content from one device to another, you can carry on using it. If you have an iPad, for example, you can send a video to Apple TV, then carry on web browsing.

Any app can support AirPlay and an extra icon should appear on your iPhone or iPad screen to let you choose to output Apple TV. Some apps don't do this, but you can manually set your iOS device to send video to the Apple TV by default*(see page 72)*.

There's no doubting the slickness, quality and ease of use of Apple TV. With 1080p support and access to your iTunes TV shows, plus Netflix built in, it's an attractive proposition at the price. If you have an iPhone or iPad, it's even better, as AirPlay lets you send your content directly to Apple TV, thus overcoming quite a few of its limitations.

How to use AirPlay

When it came to providing a way to play music, videos and photos over a network, Apple didn't want to use UPnP like everyone else, so it came up with AirPlay. The idea behind it is simple: you beam data from one device to another, so you can watch or listen to the content of your choice on the device of your choice.

For AirPlay to work, you need two things. First, you need an AirPlay-compatible device to do the beaming. This can be an iPhone, iPod Touch or iPad, although Macs also support the technology. Windows devices have poor support for AirPlay, though iTunes also supports the technology. For Android devices, you need an AirPlay-compatible app, such as DoubleTwist (http://tinyurl.com/doubletwistandroid). Note that Android apps only let you play media you own and don't add AirPlay into other apps, such as those for catch-up TV.

Next, you need a receiving device. This can be capable of video, such as Apple TV, or audio, such as AirPlay-compatible speakers. With AirPlay speakers you can use up to six at once from one device, giving you multi-room capabilities.

Before we explain how the technology works, it's important to understand that AirPlay only works with compatible files. That means that they have to be in Apple-supported video formats (such as QuickTime) and Apple-supported audio formats (such as AAC and MP3). The media provider also has to allow AirPlay; if it doesn't, you may find that you get sound, but not video, or simply nothing at all.

Rights owners can also disable AirPlay support, preventing you from beaming audio and video to a device. For example, some of the catch-up TV services only allow you to watch on your mobile device and disable AirPlay streaming. If this is the case, for video content you'll see a message on your TV telling you that the content isn't supported.

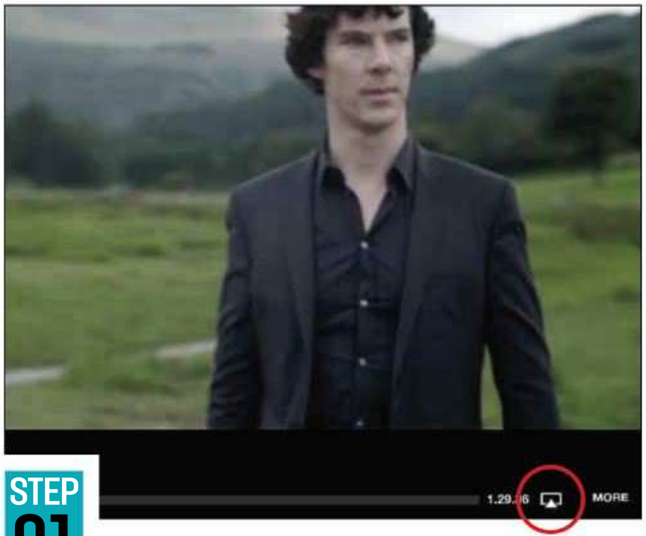
There are three modes available. In-app AirPlay lets you send the content you're currently listening to or watching to a device. This is the purest mode, as you can carry on doing something else or even turn off the screen on your iOS device. In this way, you can use your iOS device as a kind of remote control to select the media you want. You can also use the AirPlay device's remote control for playback control, including play/pause, fast-forward/rewind and track skip.

Second, all iOS devices have a system-wide setting that sends any media to a compatible device, regardless of the particular app. You can think of this as an override for applications that don't have built-in AirPlay support. For example, the BBC iPlayer app supported AirPlay, but it didn't have support built in (the new version has fixed this), so you could use the override setting instead.

Finally, there's AirPlay mirroring for iOS and OS X, which lets you mirror your device, sending video and sound to an Apple TV. This means you can use your TV as the screen to show everything that's going on, such as showing a game that you're playing. This mode can let you watch video content from apps, whereas using the other methods only gets you audio. However, content owners can disable this mode.

The latter two modes require you to keep your devices on, and you can't use them for anything else, otherwise it interrupts playback. This means your device also has to have its screen on, so it affects battery life, too.

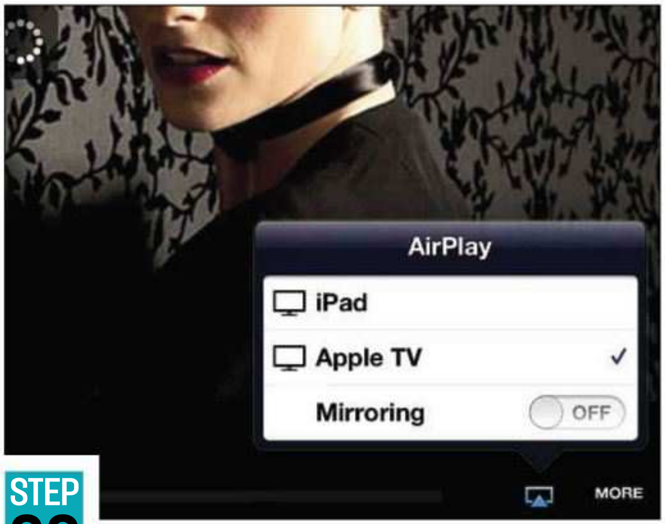
With that explained, here's how to use AirPlay. We're using an iOS device, but it's roughly the same for OS X, which uses the same icons and options.



STEP 01

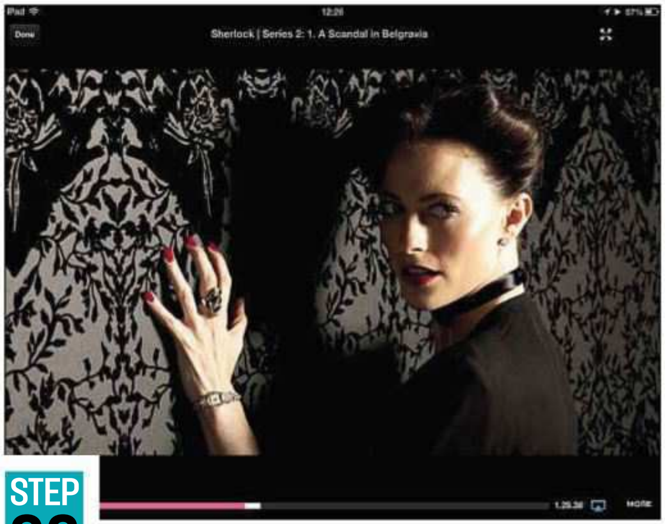
LOOK FOR ICON

First, you need to connect your playback device to the same network as your AirPlay device. Next, when you play any media using an app, look for the AirPlay icon. This will usually appear at the bottom of the screen by the play controls and status bar. You may have to tap the screen to get the bar to appear. If you don't see an AirPlay icon, the app doesn't support the technology (skip to Step 4).



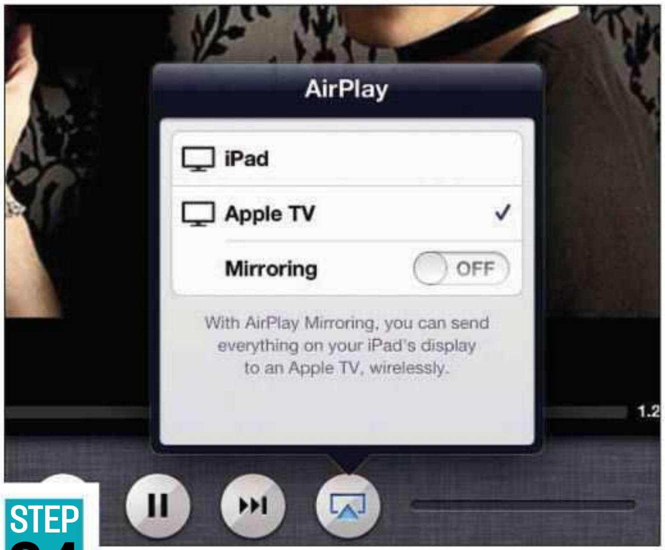
STEP 02 CHOOSE AIRPLAY DEVICE

Hit the AirPlay icon to bring up a list of AirPlay devices. Each AirPlay device can be named, following the manufacturer's instructions. If you haven't changed anything, you'll see the default name, such as Apple TV. Your media will start playing on the selected device. If you've selected an Apple TV and you're not getting video, the content you're playing isn't supported, but you can try Steps 4 and 5 as an alternative.



STEP 03 PLAYBACK CONTROLS

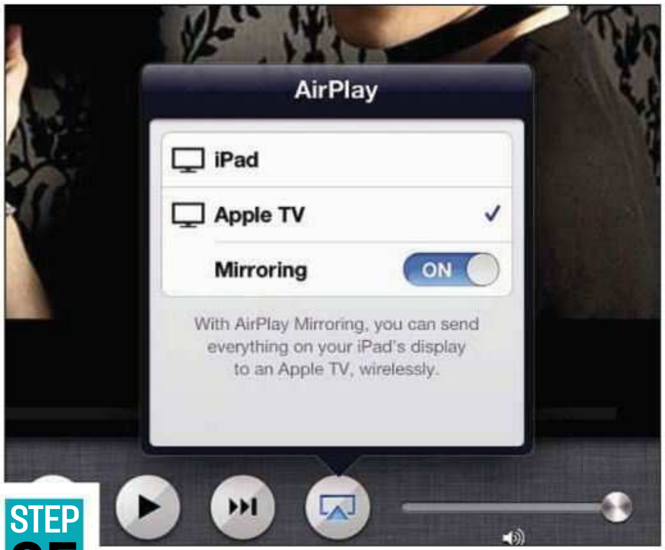
With your content playing, you can now use your playback device as a remote control. Hit Pause to stop the content and Play to continue. You can also use the status bar to scroll through the media to select a specific point in time that you want to listen to or view (this is often quicker than using the fast-forward or rewind buttons). You can also carry on using your device for any other job, and use your AirPlay device's remote control to control playback.



With AirPlay Mirroring, you can send everything on your iPad's display to an Apple TV, wirelessly.

STEP 04 SELECT SYSTEM WIDE

If your selected app doesn't have AirPlay controls, you can use the system-wide setting. Bring up the Task Switcher in iOS by double-tapping the Menu button or, on the iPad, swipe up with four fingers. Scroll to the left two screens and you'll see a volume bar with the AirPlay icon. Tap the AirPlay icon and select your playback device. All apps will now automatically send their audio and, where supported, video to the selected AirPlay device. If video still isn't working, you can skip to Step 5.

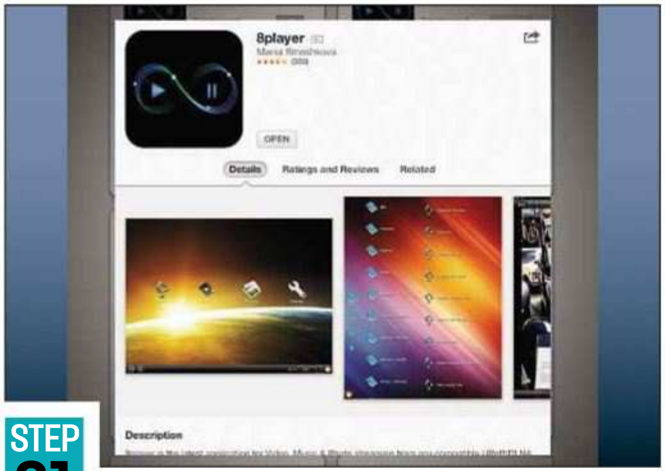


With AirPlay Mirroring, you can send everything on your iPad's display to an Apple TV, wirelessly.

STEP 05 SELECT MIRRORING

If you have an Apple TV and want everything on your device to be shown on it, bring up the Task Switcher in iOS and go to the AirPlay icon, as in Step 4. Select your Apple TV and select Mirroring. Tap Done when you're finished. You can do the same in OS X by using the AirPlay menu at the top of the screen. You'll now see your device mirrored on your Apple TV. Some video might be barred from playing, but most things will work. If you settle down to watch a video, remember that you'll have to leave it playing on your device, and you can't use it for anything else.

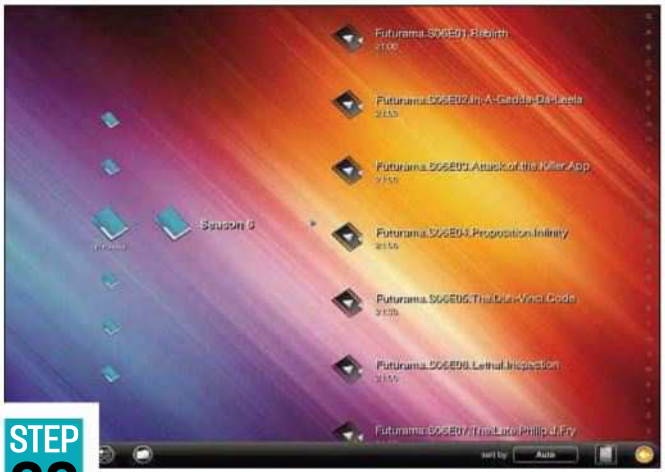
How to stream files using an iPhone or iPad



STEP 01

DOWNLOAD 8PLAYER

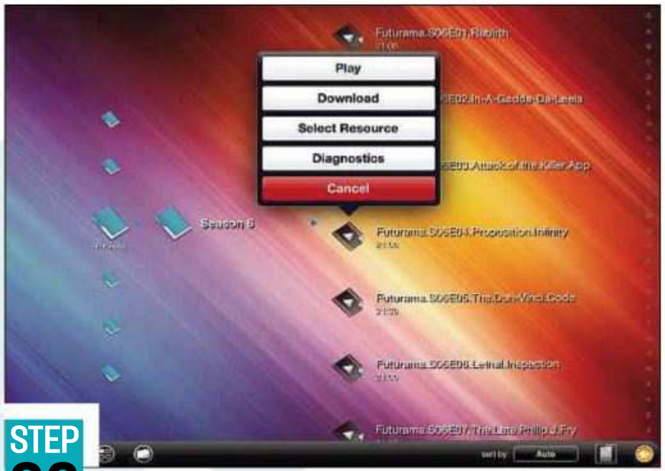
Our favourite media-playing app is 8Player. This app costs £3.99, but it's worth every penny. It will play practically any file format, connects to media servers on your home network and has AirPlay built in, so you can send what you're watching to your Apple TV or AirPlay speakers.


Futurama.S06E01.Rebirth
Futurama.S06E02.In-A-Gadda-Da-Leela
Futurama.S06E03.Attack.of.the.Killer.App
Futurama.S06E04.Proposition.Infinity
Futurama.S06E05.The.Duh-Vinci.Code
Futurama.S06E06.Lethal.Inspection
Futurama.S06E07.The.Late.Philip.J.Fry
Season 6
sort by
Auto

STEP 02

PLAY MEDIA

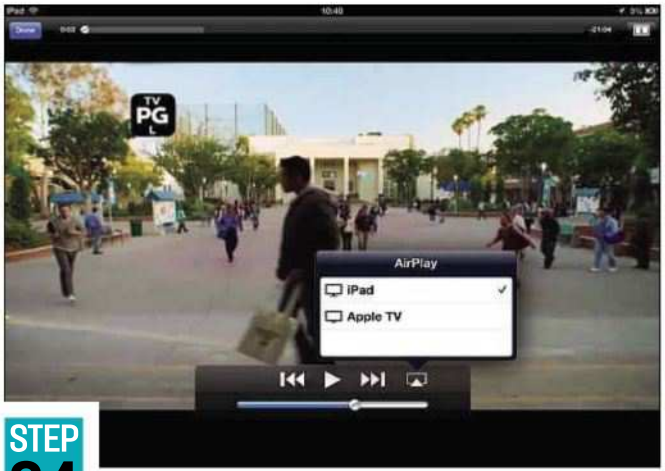
The 8Player home screen is split into three main categories: Music, Movies and Pictures. Tap the one you're interested in and you'll see a list of media servers on your home network. Select the one you want, such as your NAS, to browse through its files. You can just tap the file you want to play to start viewing or listening. You can stop at any point and, by selecting the same file again later, resume where you left off.



STEP 03

SAVE FILES

Press and hold down on a file to bring up an options menu. Play does as you'd expect, while Download saves the file to your local device. Downloaded files appear in the Download folder when you select Music, Movies and Pictures, with each having its own folder. This feature lets you save files for offline watching.

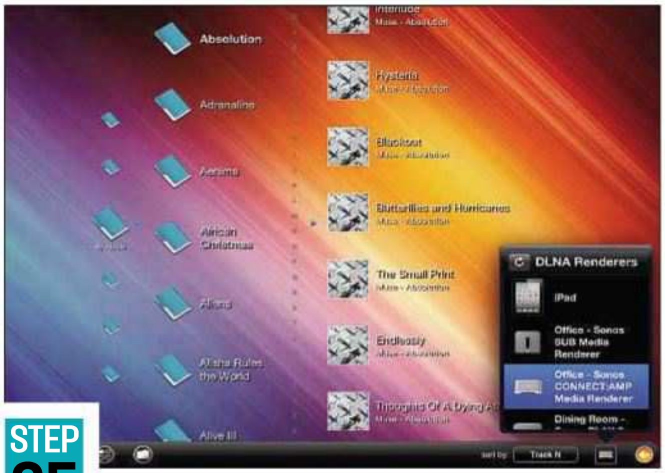


STEP 04

STREAM FILES

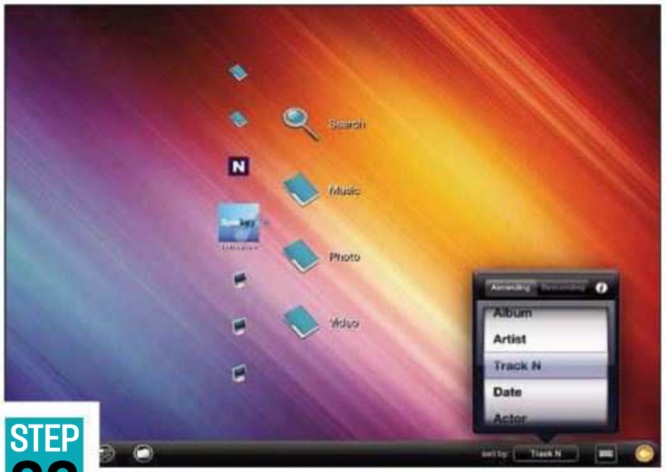
To stream a file, start playing it and tap the AirPlay icon in the play window. You can then select which device you want to send the content to. If you want to use AirPlay properly, you'll need to convert your media files to an Apple-supported format. However, 8Player supports AirPlay mirroring, so you can play any video format, although this method requires you to leave your iOS device turned on while the media is playing.

Apple likes to do things its own way, which typically means that you have to use Apple kit and Apple-supported file formats in order to view everything. That's not always very convenient, though, particularly if you have a large collection of videos or music that's been saved in a format that's not supported by your player. In this walkthrough, we'll show you how to play anything on your iPhone or iPad using the 8Player app (http://tinyurl.com/8player), which is available for £3.99 from the App Store.



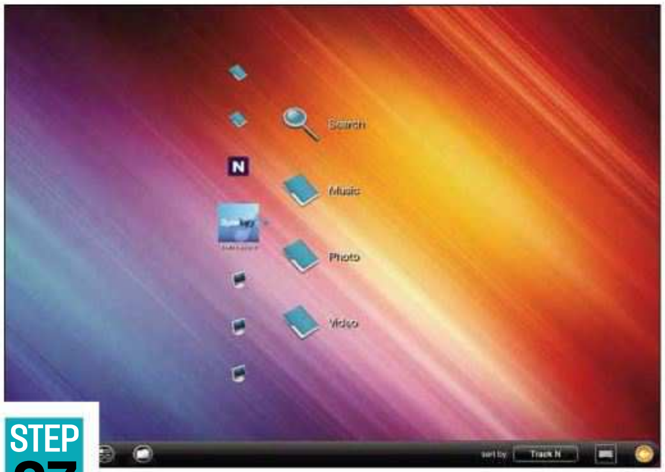
STEP 05 DLNA

8Player can also send content to DLNA renderers, such as some modern TVs and wireless speakers. Tap the Orange icon at the bottom of the screen to expand the Settings bar, then click the icon that shows your current device (iPad or iPhone). This gives you a list of DLNA renderers on your network: tap the one you want to use. You'll have to stop any media playing and resume it to send it to your chosen renderer.



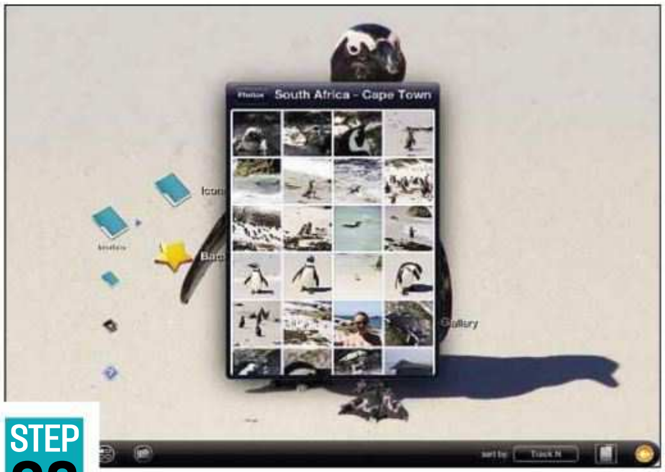
STEP 06 SETTINGS

Also on the Settings bar, you'll see a Sort by menu. This lets you change how media is organised. The default option is Auto, which sorts music tracks by name, rather than track number. To fix this, tap the list and change it to Track N. This will sort your music by track number, so that files appear in the correct album order.



STEP 07 SHORTCUTS

You can also use the Settings bar for shortcuts. The first icon is to jump straight to the current playback; the second shows you current downloads; the third takes you to the home screen; and the fourth icon is to jump straight to files you've downloaded. When you're done with the bar, you can just tap the orange icon to close it.



STEP 08 SETTINGS

Back on the home screen is a main Settings app. This has some advanced control settings, but the defaults are generally fine. However, you can use Settings to change the look and feel of the app. You can change the icon style, and change the background to use one of the photos stored on your iPhone or iPad.

7

INTERNET SECURITY

As soon as you connect to the internet, your computers are at risk from hackers. In this chapter, we'll show you how to defeat them and stay safe. We'll explain how hackers attack, how to spot scams, how to protect against malicious software and how you can filter out the bad stuff online. We'll also show you how tracking software means that you can even find and recover a stolen laptop.

CONTENTS

Googl
Micros
fac

The dark economy

There's a great deal of mythology, rumour and misinformation surrounding computer security, from urban myths about emails that will format your hard disk if you read them to fake anti-virus software that holds your PC to ransom while claiming to protect it. Being able to recognise what is and isn't likely to constitute a threat is a skill that comes with experience. The more you know about threats and how they work, the easier it is to protect yourself. In this chapter, we'll guide you through the ins and outs of security, from protecting your mobile phone to understanding what malware makers hope to gain and what you stand to lose.

While the news is filled with stories about viruses designed to disable Iranian nuclear power stations and websites being taken down by distributed denial-of-service (DDoS) attacks intended to make a political statement, the vast majority of malware and other online security threats exist to make money. From stolen credit card data to botnets, a huge underground economy has been built upon cybercrime, and it costs the UK an estimated £27 billion per year.

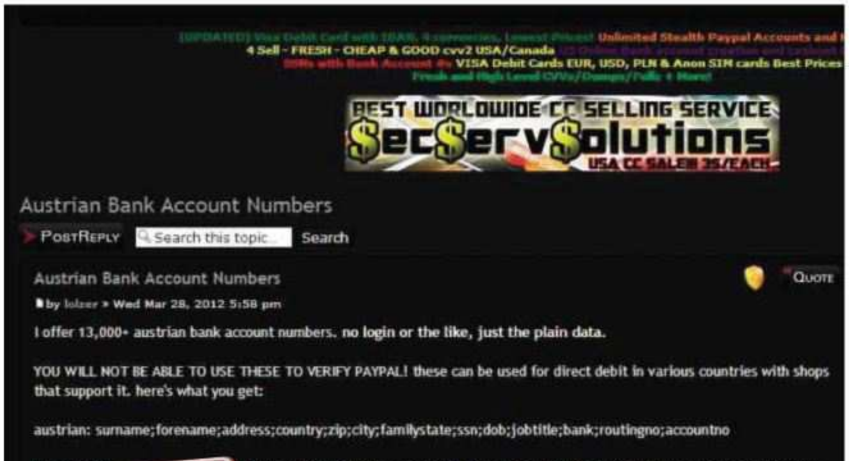
> “A huge underground economy has been built upon cybercrime, and it costs the UK £27 billion per year.”

DIFFERENT STROKES

As with any supply and demand economy, various roles have sprung up within the shadowy world of cybercriminals, from programmers who produce and sell the malware, to botnet operators who remotely command a network of 'zombie' computers, and credit-card fraudsters who buy card numbers harvested by malware and sold in batches on underground message boards.

The terminology used is deliberately arcane, but the relationships and transactions involved aren't very different to those of more mundane criminal operations, or even legitimate businesses. The malware industry has become so professional, in fact, that it's not uncommon to see adverts from companies looking to hire malware coders on the underground forums that are a cornerstone of the industry.

The malware industry is a form of organised crime that's far removed from the old image of hackers as curious teenagers



Unlimited Stealth Paypal Accounts and

4 Sell - FRESH - CHEAP & GOOD cvv2 USA/Canada

VISA Debit Cards EUR, USD, PLN & Anon SIM cards Best Prices

Fresh and High Level CVVs/Dumps/Fulls + More!

Austrian Bank Account Numbers

Austrian Bank Account Numbers

by lolzer » Wed Mar 28, 2012 5:58 pm

I offer 13,000+ austrian bank account numbers. no login or the like, just the plain data.

YOU WILL NOT BE ABLE TO USE THESE TO VERIFY PAYPAL! these can be used for direct debit in various countries with shops that support it. here's what you get:

austrian: surname;forename;address;country;zip;city;familystate;ssn;dob;jobtitle;bank;routingno;accountno

these can b osit fraud or for sites that need you to enter a valid bank account. many shops in germany a ts even for first orders, albeit only for low value orders, up to around 100 or 200 EUR. amazon

Dedicated forums, often on hidden networks, are used to discuss hacking techniques, sell stolen data and advertise services and tools from malware coders

playing pranks on authority figures. As with any industry, there are a number of roles and relationships. Here we take a look at a few of them to help provide a picture of how the malicious software industry works.

MEET THE CODERS

Malware coders create and sell malicious software to criminals. It's often claimed that the creator of the software technically isn't doing anything illegal because they don't use it themselves to commit any crime. However, recent arrests of malicious software developers indicate this isn't regarded as much of an excuse by the authorities. It remains common to sell malware tools for 'testing' or 'reference' purposes only. Large-scale malware production is common, too, with coders hired by organised criminal gangs.

Examples of malicious software include tools to capture information typed into forms on an infected PC, fake anti-virus software that locks your PC and demands money to 'register' it, and botnet clients that remotely control the networking capabilities of the PCs they're installed on so they can be used as part of a DDoS attack. These tools are often bought by less technically minded criminals who use them to extract money or saleable data from their targets.

DISTRIBUTORS AND OPERATORS

Once the malware has been bought, its new owner needs to infect PCs with it – and there are a few ways of doing this. We explain threat vectors in more detail on page 78, and some infection methods are bought and sold as services. Most common of these include web-based drive-by downloads, concealing links to malware within spam emails and using botnets to copy malware on to an already compromised PC.

Drive-by download distributors spread their malicious software using the web, often via unwitting advertising networks. They can also set up sites as a front to distribute the malware; pornography is popular, as it attracts a wide audience of often distracted victims who may be unwilling to discuss the source of their malware infection with the authorities. Another option is to use cross-site scripting to make a browser load malicious code into harmless websites, from which it can be spread further. Whichever method is used, the drive-by site will attempt to install malicious software on any vulnerable PC that visits it.

Most banks now use two-factor authentication devices that generate a second, one-time password to prove a user's identity

Botnet operators control a network of computers that have been infected with botnet client software. These machines are typically hired out to carry out DDoS attacks to knock out websites, send bulk email spam, combine the PCs' processor power to carry out brute-force password cracking or distribute other malicious software.

Malware commonly captures data, such as usernames and passwords or financial details. To this end, PCs are infected with programs such as keyloggers, which capture what you type. Even harder to foil is malware that uses techniques known as 'man-in-the-middle' and 'man-in-the-browser' attacks. These allow the malware to eavesdrop on data you send to a website without the knowledge of either you or the site.

Some programs do even more. Tatanga, for example, a man-in-the-browser Trojan that targets customers of German banks, waits for you to log into an online banking service it recognises, chooses one of your accounts and initiates a transfer. It then pops up a window asking the user to generate a PIN code on the hardware authentication device in the guise of a test being made by the bank. If the user falls for this, Tatanga can then transfer money out of the account.

Like most financial malware, Tatanga is very specifically targeted. However, the use of cleverly designed malware with social engineering elements to fool its victims is likely to spread.

Even if the criminals responsible for the malware infecting a PC don't steal their victims' money directly, credit card details, webmail logins, online gaming account details and more can be captured and then sold in online markets, where they're bought by people keen to defraud you and who require little technical skill themselves to go about doing so.

Threat vectors

Your PC doesn't exist in a vacuum. Email, websites and removable media can all provide malicious software with the means to get on to your system. Here are several common approaches used by the bad guys to infect your network.

EMAIL

Malware used to be most commonly spread via email, either in the form of mass spam or a message sent from the account of a friend whose PC had already been compromised. Emails would usually have an executable attached and text enticing you to run it.

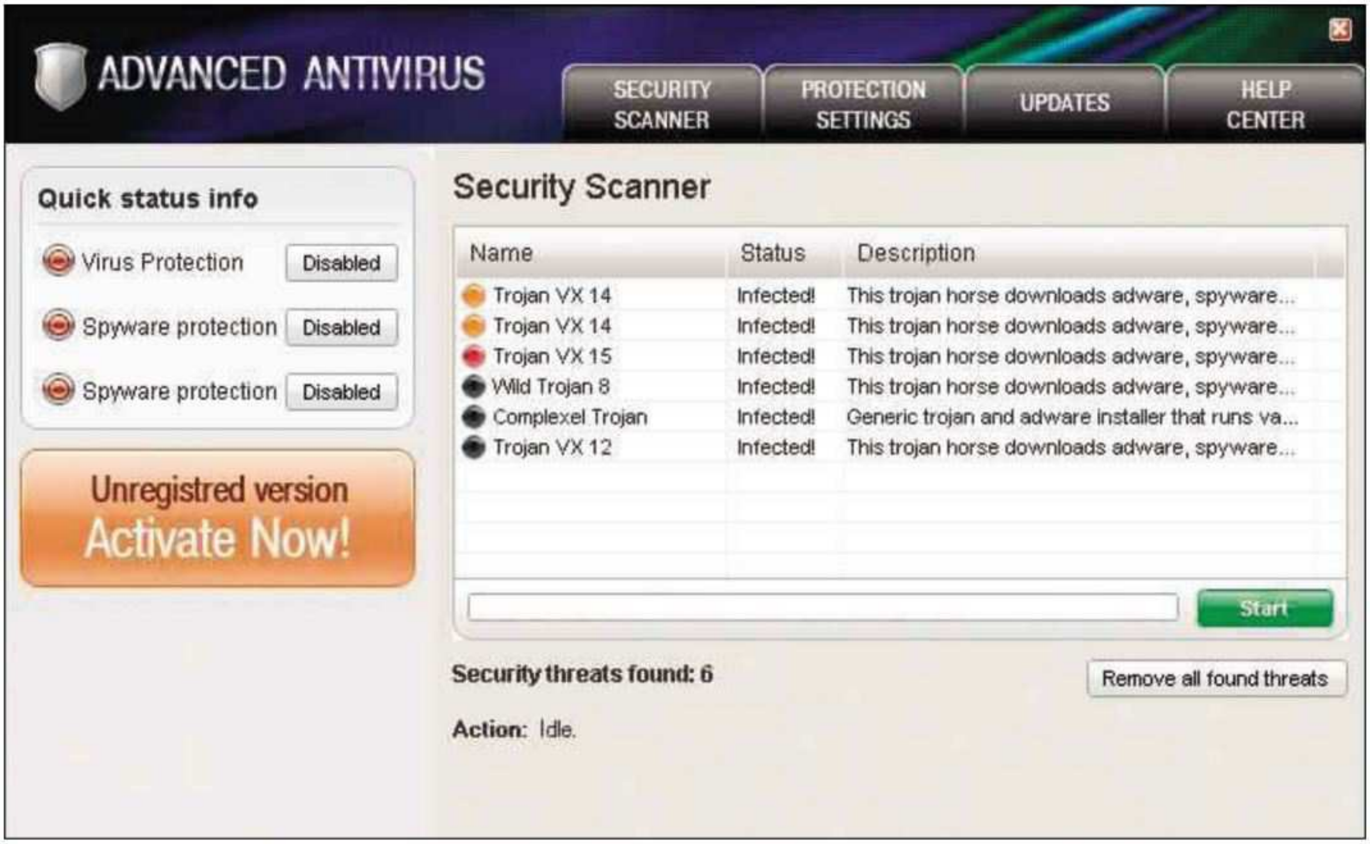
Malicious attachments are still used, but most people now know better than to run an attachment sent from an unknown source. The rise of web-based email services, such as Gmail and Hotmail, with integrated virus scanning that blocks or removes unsafe content, has also made this method of infection less common.

These days, malicious emails are more likely to contain links that send you to a site that will attempt to carry out a drive-by download. Such emails also use elements of social engineering (*see page 82*), often claiming to provide links to news stories about dramatic current events.

Autorun malware, which takes advantage of Windows' automatic loading of a hidden Autorun.inf file, is commonly spread by infected USB drives

AUTORUN

This well-established type of worm is still widespread, despite the release of operating system patches to combat it. It uses Autorun.inf files, which can be put on a disc or USB stick, to make Windows automatically carry out the instructions in the file. This typically involves running a malicious executable hidden elsewhere on the storage media. The malware, once on your system, will typically try to copy itself to any USB storage device that you connect to your PC.



Quick status info

Virus Protection	Disabled
Spyware protection	Disabled
Spyware protection	Disabled

Security Scanner

Name	Status	Description
Trojan VX 14	Infected!	This trojan horse downloads adware, spyware...
Trojan VX 14	Infected!	This trojan horse downloads adware, spyware...
Trojan VX 15	Infected!	This trojan horse downloads adware, spyware...
Wild Trojan 8	Infected!	This trojan horse downloads adware, spyware...
Complexel Trojan	Infected!	Generic trojan and adware installer that runs va...
Trojan VX 12	Infected!	This trojan horse downloads adware, spyware...

Security threats found: 6

Action: Idle.

Fake anti-virus software is one of the most common types of drive-by downloads. After it's taken control of your browser, it will report scores of non-existent viruses, lock up your PC and demand a 'registration fee' from its victims

> "Unfortunately, avoiding drive-by downloads isn't as simple as staying away from dodgy sites. This kind of threat is often found in banner adverts."

DRIVE-BY DOWNLOADS

The most common way you'll encounter malware in the wild is via a drive-by download. These attacks are embedded in the code of a website and will try to use your browser to download and run a malicious file on your computer. Unfortunately, avoiding drive-by downloads isn't as simple as staying away from dodgy sites.

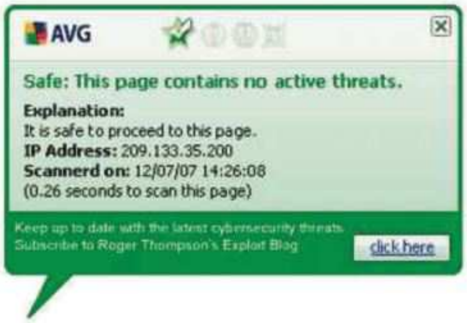
This kind of threat is often found in banner adverts that open content from a third-party site; an innocent example is adverts that show products from John Lewis you've recently browsed.

The owner of the site on which they're displayed usually has no control over the content of advertising iframes (named after the HTML tag in which they're enclosed). This is how even well-known sites such as MySpace have unwittingly exposed their users to malware in the past. Other common tactics include installing an Internet Explorer ActiveX plug-in, running malicious Java code or simply saying you need to download special software to view content on the page.

As advertising providers have become wise to the tactics of malware distributors, it's become a little harder for virus makers to embed their malware in legitimate websites, but insecure websites can often still be exploited using cross-site scripting attacks that inject malicious code into a website without its owner's knowledge.

INFECTED SOFTWARE

If you download pirated software via file-sharing sites of any sort, there's a chance that it will contain malware in addition to or instead of the program you thought you were getting. It's also worth noting that the cracking tools supplied with many bootlegged games are often picked up as malware by anti-virus software, making it difficult to tell what level of



Safe: This page contains no active threats.

Explanation:
It is safe to proceed to this page.
IP Address: 209.133.35.200
Scannerd on: 12/07/07 14:26:08
(0.26 seconds to scan this page)

Keep up to date with the latest cybersecurity threats
Subscribe to Roger Thompson's Exploit Blog

Browser protection plug-ins can let you know if a web page or search result is safe or not, but it's still important to watch for suspicious links before you click

threat the program actually represents. For this reason, among many others, we strongly advise against using pirated software.

SOCIAL ENGINEERING

Social-engineering attacks are the broadest category of online threats. Rather than trying to get a malicious program on to your PC or using brute force to crack email passwords, social-engineering attacks instead use deception to target the user directly, trying to get them to give away passwords and personal data unwittingly. It's basically a very fancy name for a rather traditional con.

Social-engineering attacks range from generic 'phishing' emails and websites that use logos and lookalike links to convince you they come from your payment provider, to people who phone up claiming to be from Microsoft to get you to give them money or install remote-access software on your PC. There are even precisely targeted scams tailor-made to con key staff at business and financial institutions.

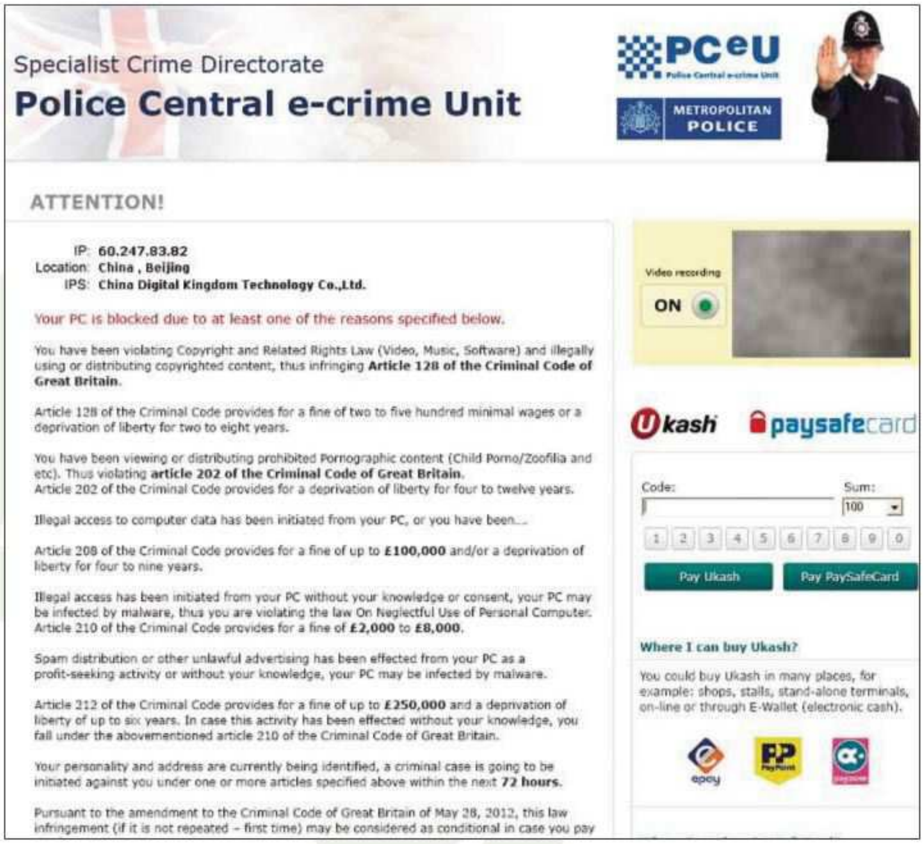
While some internet security programs can flag up phishing sites, being well informed about security and knowing what to watch out for are the best defences against you becoming the weak link in your own computer security system.

It's worth repeating here that Microsoft will never ring you up to discuss problems with your PC, and that the former member of the Egyptian government certainly does not have a million pounds for you. See our social-engineering defence kit *(page 82)* for more tips on what to watch out for.

SOCIAL MEDIA

With everyone and their cat now on social media, it was only a matter of time before Facebook and Twitter became key threat vectors. Once again, these are essentially drive-by downloads with a bit of social engineering to help them spread. However, additional vulnerabilities and characteristics of the most popular social networks are often exploited to make the malware distributors' lives easier.

These include 'likejack' tactics, hidden Facebook Like buttons that are set off when you click on something else and publish content to your wall without your knowledge – and so use your good name to promote unsafe content. Meanwhile, beware of giving third-party applications or sites access to your Twitter account, as these can post messages on your behalf, including malicious links. This means even content on your friends' social-networking profiles can't necessarily be trusted to be trouble-free.



Specialist Crime Directorate
Police Central e-crime Unit

ATTENTION!

IP: **60.247.83.82**
Location: **China , Beijing**
IPS: **China Digital Kingdom Technology Co.,Ltd.**

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing **Article 128 of the Criminal Code of Great Britain**.

Article 128 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating **article 202 of the Criminal Code of Great Britain**.
Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access to computer data has been initiated from your PC, or you have been...

Article 208 of the Criminal Code provides for a fine of up to **£100,000** and/or a deprivation of liberty for four to nine years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of **£2,000** to **£8,000**.

Spam distribution or other unlawful advertising has been effected from your PC as a profit-seeking activity or without your knowledge, your PC may be infected by malware.

Article 212 of the Criminal Code provides for a fine of up to **£250,000** and a deprivation of liberty of up to six years. In case this activity has been effected without your knowledge, you fall under the abovementioned article 210 of the Criminal Code of Great Britain.

Your personality and address are currently being identified, a criminal case is going to be initiated against you under one or more articles specified above within the next **72 hours**.

Pursuant to the amendment to the Criminal Code of Great Britain of May 28, 2012, this law infringement (if it is not repeated – first time) may be considered as conditional in case you pay

Code:
Sum: 100

Where I can buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash).

Some of the most shameless social engineering attacks claim to have detected illegal activity on your PC, lock your system and demand a 'fine' to release it

BITDEFENDER'S BIGGEST THREATS

01 TROJAN.AUTORUNINF

Even though Windows' autorun vulnerability hasn't been present since the release of Windows 7 in 2009 and has been patched in security updates for older version such as Windows Vista and XP, this generic class of Trojan remains massively common. It spreads by taking advantage of Windows' automatic handling of Autorun.inf files on infected USB drives and frequently comes with, or attempts to download, additional malware.

PERCENTAGE OF MALWARE DETECTED: 4.66%

02 ADWARE.SOLIMBA

This is generic detection classification that indicates that an installer is attempting to install potentially unwanted third-party software in addition to the program the user actually wants. The maker of the installer is paid to include these extras. Rarely harmful but often annoying, junk browser toolbars are common unwanted additions.

PERCENTAGE OF MALWARE DETECTED: 4.41%

03 EXPLOIT.CPLLNK.GEN

Commonly used by the notorious Stuxnet worm, which was originally designed in 2010 to attack Siemens' industrial controllers used by Iranian nuclear power facilities, this exploit takes advantage of a vulnerability in the way in which Windows handles lnk shortcut files to execute malicious code.

PERCENTAGE OF MALWARE DETECTED: 3.54%

04 WIN32.WORM.DOWNADUP

Also known as Confiker, Downadup is a worm that joins infected computers to a botnet that is still flourishing five years after it was initially detected in 2008. Different versions of the worm have exploited a range of Windows vulnerabilities to propagate, including NetBIOS and Autorun issues.

PERCENTAGE OF MALWARE DETECTED: 3.13%

05 JS:TROJAN.SCRIPT.EY

Targeting browsers, this Trojan injects its own JavaScript code into entirely innocuous HTML files, redirecting the user to a malware-bearing website, from which further infection will commence.

PERCENTAGE OF MALWARE DETECTED: 3.11%

Social engineering defence kit

Your guide to spotting the scams

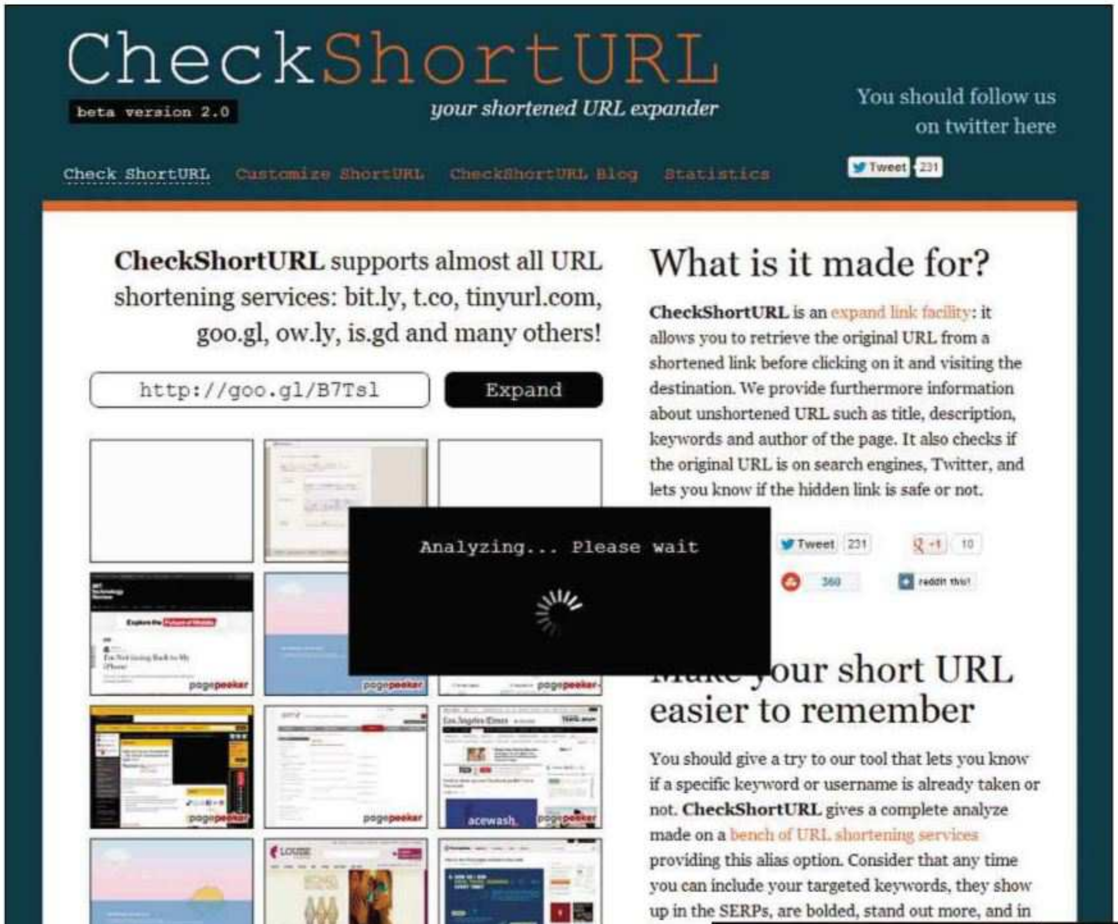
Watch out for emails claiming to be from your bank or from popular online retail or payment services such as eBay, especially if they appear to be warnings that your account is about to be frozen. Always visit financial sites directly, by typing their URL into the address bar of your browser, rather than clicking on a link in an email.

While grammar obsessives may be the bane of internet debate forums everywhere, it's worth bearing in mind that legitimate emails and websites from your bank or other businesses will use correct English. Watch out for characteristic mistakes in tense or pronoun gender made by writers who don't have English as a first language, as many of these scams originate from outside the UK.

> "When using social media, watch out for teaser links on friends' walls designed to tempt you into clicking."

It's common for spam to use disguised links to trick readers into visiting malware-bearing sites. Hovering your mouse over a suspect link will show you the URL it goes to at the bottom bar of your browser or email client. If it doesn't match up with what it claims to be, don't click on it. Always use up-to-date web browsers and email clients, as they're less vulnerable to tactics that can be used to further obscure links. If you're sent a shortened URL, you can check it before you open it at www.checkshorturl.com.

When using social media, watch out for teaser links on friends' walls designed to tempt you into clicking on them. Popular content for such links include offers of free vouchers, apps that claim to show you who's been viewing your profile or saucy pictures with captions such as "I can't believe she did THAT!" Also beware of messages that claim to have photos of you in a compromising situation accompanied by a shortened URL. Don't share too much personal information about your home address, travelling habits, work details, date of birth and so on; the friendly-looking person who sends a friend request because you both play Farmville could be a scammer looking for personal data.



CheckShortURL supports almost all URL shortening services: bit.ly, t.co, tinyurl.com, goo.gl, ow.ly, is.gd and many others!

http://goo.gl/B7Tsl

What is it made for?

CheckShortURL is an expand link facility: it allows you to retrieve the original URL from a shortened link before clicking on it and visiting the destination. We provide furthermore information about unshortened URL such as title, description, keywords and author of the page. It also checks if the original URL is on search engines, Twitter, and lets you know if the hidden link is safe or not.

Make your short URL easier to remember

You should give a try to our tool that lets you know if a specific keyword or username is already taken or not. CheckShortURL gives a complete analyze made on a bench of URL shortening services providing this alias option. Consider that any time you can include your targeted keywords, they show up in the SERPs, are bolded, stand out more, and in the mea

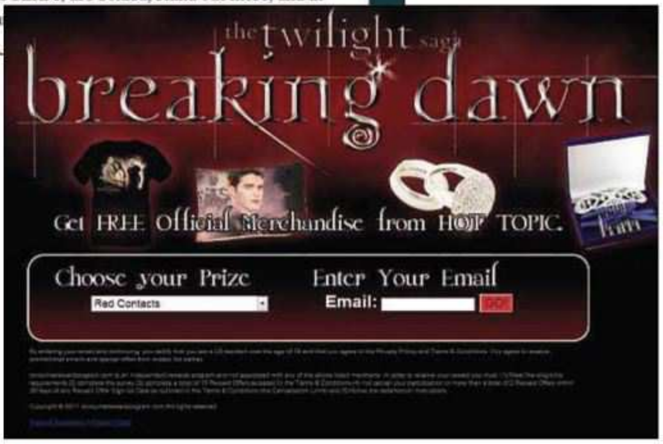
If you're sent a shortened URL from a suspicious or unknown source, you can check it at www.checkshorturl.com to make sure it redirects you to a safe site

If someone phones you up claiming to be from Microsoft and saying there's a problem with your PC, they're lying. In fact, the same applies to anyone cold-calling you about your computer or its security.

No police force operates by fining you over the internet or locking up your PC until you pay them. Rest assured that if you really were implicated in a sting operation against child pornography, zoophilia or something equally vile, you would not be hearing from the police via a browser pop-up. This form of 'ransomware' can be detected and removed by most anti-malware tools.

Beware fake anti-virus messages. If you visit a site and a pop-up from an unknown anti-virus utility appears on your screen, don't click on anything and close your browser by right-clicking its taskbar icon and selecting 'Close window'. Run legitimate anti-virus software as soon as possible.

Surprisingly convincing fake anti-virus programs will claim your PC is heavily infected with malware, as well as prevent you accessing Safe mode or installing real anti-virus software. They then insist that you pay for a 'full' version of the fake AV software. Never pay for this kind of ransomware.



Scammers and malware distributors take advantage of popular trends to harvest personal data and convince users to click through to malware-bearing sites

Business concerns are beyond the scope of this feature, but it's worth bearing in mind that staff may be targeted by frauds trying to get them to share data or passwords. Educate them to make sure they know who they're talking to on the phone or via email before they share any critical information. Just because someone claims to be from your company's external IT support contractor doesn't mean they actually are.

Security manual

It's easy to think of computer security as a kind of technical problem that's solved by installing anti-virus software, but assessing your real security needs is easier if you think about it in more concrete terms. Most of us are concerned about three key things:

1. **Theft or loss of hardware**
2. **Theft or loss of data, including content such as photographs, documents and private emails**
3. **Theft of account information such as webmail or banking data.**

Many of these can be interlinked; the loss of a smartphone, for example, would most likely cover all three of these categories if you had personal photos on it and also used it to access retail or banking sites. We've also included a section on content filtering *(see page 92)*, so you can prevent children or others using your PC to access unsuitable material.

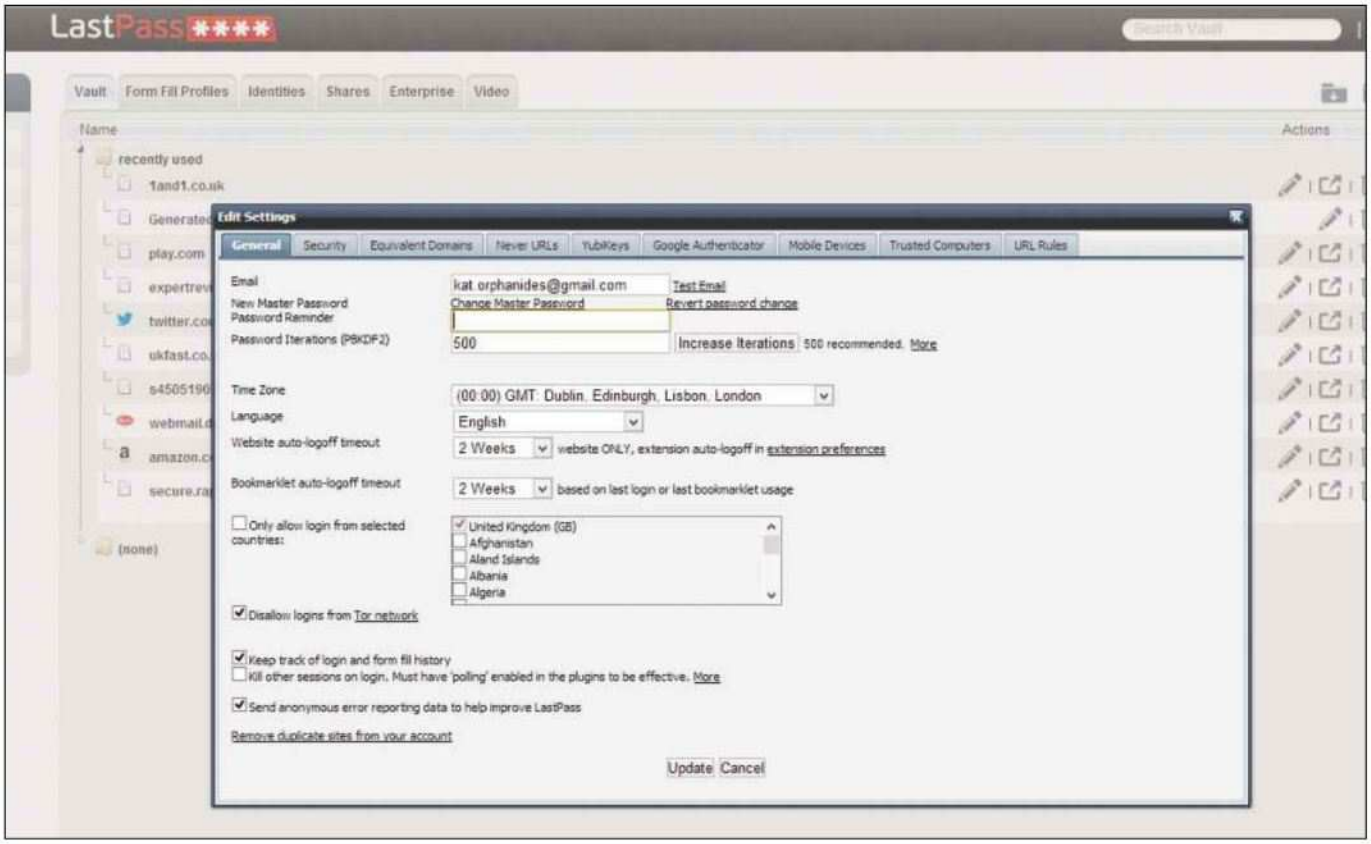
For most of us, our initial thoughts upon losing a device are for the device itself – if it was stolen, it was probably the primary target of the thieves, rather than its contents. Now we're not going to tell you how to keep a hold of your kit, but on page 98 we look at what you should do if you lose a device – with an eye to tracking it down, rendering it useless to thieves and making a claim on any insurance you might have.

The data contained on the device, such as photos, may be irreplaceable and possibly far more valuable to you. If you use your laptop for work, then the data it holds could be of interest to financial criminals or business rivals. If your video of your child's first steps is on your phone when it's stolen, then it's probably gone for good. And most gamers aren't going to be at all happy if they try log into their MMORPG account to find that it's been stolen by someone who's going to abscond with all their gold and fancy items.

Being aware of your needs in terms of physical, data and account security will help you find effective strategies for protecting yourself and minimising the impact if anything does go wrong. On the following pages, you'll find our guides to everything from installing PC security software to keeping track of your mobile phone.

ACCOUNT SECURITY

While having to reformat your computer or replace a mobile phone are both troubling wastes of time and quite possibly money, the consequences of having your personal information stolen can haunt you for years. Some of us store enough



Email: kat.orphanides@gmail.com Test Email

New Master Password: Change Master Password Revert password change

Password Reminder:

Password Iterations (PBKDF2): 500 Increase Iterations 500 recommended. More

Time Zone: (00:00) GMT: Dublin, Edinburgh, Lisbon, London

Language: English

Website auto-logoff timeout: 2 Weeks website ONLY, extension auto-logoff in extension preferences

Bookmarklet auto-logoff timeout: 2 Weeks based on last login or last bookmarklet usage

□ Only allow login from selected countries:
☑ United Kingdom (GB)
□ Afghanistan
□ Aland Islands
□ Albania
□ Algeria

☑ Disallow logins from Tor network

☑ Keep track of login and form fill history
□ Kill other sessions on login. Must have 'polling' enabled in the plugins to be effective. More

☑ Send anonymous error reporting data to help improve LastPass

Remove duplicate sites from your account

Update Cancel

Using a password manager such as LastPass means that you have to change only one password to resecure most of your accounts

personal information on our phones and computers to give an enterprising thief a big head-start in defrauding us.

Some people prefer to enter passwords for services – such as email and Facebook, as well as Amazon and banking – every single time they access them. This is a good idea, but if you use these services many times a day, it's understandable that you might want them stored for convenience, so most of us do so with at least some of these sites.

If you've lost a device, or found out that one or more of your online accounts or services has been compromised, then you should move quickly to resecure them. Changing the passwords to your key online accounts is an essential first step. If you've been using Gmail for years and stored the password in your browser, a thief will have access to your complete archive of email until you change the password.

> “Some of us store enough information on our phones and PCs to give an enterprising thief a big head-start in defrauding us.”

A long-term Gmail user could have legitimately sent personal emails including everything from their passport number to their home address, received emails about genealogy search results on their mother's maiden name and any number of other critical pieces of identity information. Saved browser passwords are a goldmine to someone who may want to impersonate and defraud you. Many companies like to call this 'identity theft', but we think that sounds a bit overdramatic.

The best option is not to save your passwords at all, especially in a web browser. Most browsers will happily reveal all stored passwords at the click of a Settings menu option. However, keeping track of the scores of registrations we're prompted to make online is a lot to ask of anyone's memory, especially if you follow best practice and use different passwords for each one.

Our preferred option for securing online account data is to use a password-management tool such as LastPass (www.lastpass.com), a free service that works with all major browsers and mobile devices. It supports two-factor authentication, which requires a second proof of identity (such as a fingerprint or authentication message from your smartphone) to verify your password. We recommend configuring LastPass to log you out every time you close your browser for optimal security. Some other services, including Gmail, also support two-factor authentication, which provides a valuable extra layer of protection.

Using a password manager such as LastPass isn't completely airtight, but it will make the process of resecuring your accounts in the event of a security breach quicker and easier. Bear in mind that services with installable components such as Microsoft SkyDrive and Dropbox typically remain logged in via the local application, so you may need to address those individually from their web interfaces.

WHATEVER THE ISSUE, YOU CAN REPORT IT RIGHT HERE
Report a Problem

You should report any suspicious activity immediately

ACCOUNT RECOVERY

If the worst happens and your personal accounts are compromised, your first step should be to consider whether they provide access to any financial data. While this obviously applies to your internet banking passwords and security keys, you should also consider whether other accounts could affect your banking security.

For example, do you keep a banking PIN code stored in the guise of a phone number in your Google Contacts, or have you ever sent credit card details in a plain text email? If so, it's best to change the PIN and – if you think there's any risk of the data being used – inform your bank immediately. Bear in mind that being careless with your personal financial information can invalidate any fraud protection schemes that may normally apply to bank accounts and credit cards.

> "Being careless with your personal financial information can invalidate any fraud protection schemes that normally apply to bank accounts and credit cards."

In the case of social media and email accounts, your first step is to attempt a recovery login using the phone number, emergency email address or personal data that you set up when you created the account. If that doesn't work, your best recourse is to contact the provider of your email or social media account with as much information as you can about when you last logged into the account, including your old password and anything you might know about a potential security breach. Be patient in waiting for a response and be aware that you may have to provide additional evidence of your identity and your ownership of the account. Some service providers may be more helpful than others.

USEFUL LINKS AND CONTACTS

Microsoft account recovery
https://account.live.com/password/reset

eBay account recovery
http://tinyurl.com/EbayRecovery

Facebook account recovery
https://www.facebook.com/hacked

Google account recovery
https://www.google.com/accounts/recovery

Yahoo! account recovery
https://edit.yahoo.com/forgotroot

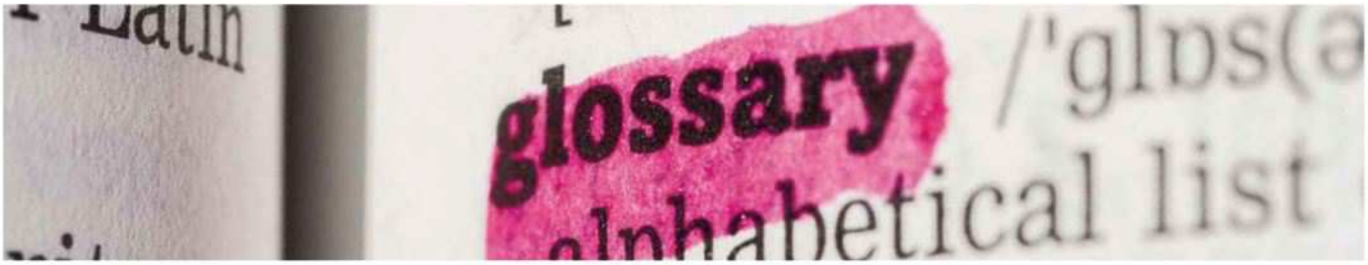
Twitter account recovery
https://support.twitter.com/articles/185703

PayPal suspicious activity
http://tinyurl.com/PayPalRecoveryUK

Yahoo! security contact address
account-security-help@cc.yahoo-inc.com

Apple ID account recovery
http://tinyurl.com/appleidrecovery

GLOSSARY: DECODING MALWARE JARGON



If you read about malicious software online, you'll find yourself learning a new vocabulary. We've touched elsewhere on the different kinds of malware you might encounter, but here we explain a few more terms that crop up regularly.

Backdoor A program that allows a computer to be secretly accessed by a remote attacker.

Black hat/white hat Just like old westerns where the sheriff wears a white hat and the villains are in black, hackers are often divided into 'black hat' and 'white hat' groups – or at least they are by their own community, possibly over-romanticising the whole thing.

Black hat hackers break security for personal gain or malicious purposes, while white hat hackers do the same thing but are paid by companies to test security and make sure hackers with bad intentions can't access their systems.

Many hackers in practice fall into the murky middle ground between the two; these are called 'grey hat' hackers. While most grey hat hackers don't get involved with blatantly malicious or illegal activities, they may be entirely willing to announce vulnerabilities that major software firms would like to keep secret, or participate in 'hacktivism' – targeted attacks against companies or governmental organisations with activities to which they're ideologically opposed. Of course, such activity can be illegal in and of itself.

Botnet A network made up of compromised PCs that can be controlled remotely *(see 'Zombie')*.

Cross-site scripting (XSS) A malicious attack that takes advantage of vulnerabilities in applications such as web browsers in order to embed malicious content in a benign site as it's being rendered by unsuspecting users.

DDoS A denial-of-service (DoS) attack occurs when a system, program or server is prevented from working, generally by overloading it with queries. Distributed denial-of-service (DDoS) attacks occur when multiple systems are involved in creating this overload. A popular use of this tactic occurs when multiple PCs repeatedly load content from a web server in order to knock it offline or render it unresponsive to genuine queries. DDoS attacks are often carried out by botnets *(see above)*.

Heuristic detection A tactic used by anti-virus software to identify entire classes of malware based on rough characteristics of code and behaviour. This method is particularly used to detect polymorphic viruses *(see 'Obfuscation')*, which don't retain a consistent signature with which they can be identified.

Keylogger Software that captures the keystrokes typed on an infected machine, such as website passwords. Will typically report these back to its owner, along with the context in which they were used.

Man-in-the-middle attack Data theft carried out by malicious software that inserts itself between the user and the location to which they're sending data.

Obfuscation In order to avoid detection by anti-virus software and analysis by malware researchers, the code of malicious programs is often made deliberately difficult to interpret, often by encrypting chunks of code that are then decrypted on the fly as the malware runs. Polymorphic malware is capable of changing its code (but not its functionality) every time it reproduces itself, so that no two iterations have the same hash signature.

Penetration testing Carried out by white hat hackers, penetration (or pen) testing simulates an attack on a network or system from outside in order to assess its security.

Ransomware Malware that locks the target PC and demands payment to release it. The most common form of ransomware is fake anti-virus software.

Trojan A malicious program disguised as or embedded in another program.

Worm A malware capable of replicating itself, for example by copying itself on to network shares, removable media or email attachments.

Zombie A computer that's been infected by a backdoor or botnet client so that it can be controlled remotely.

Securing your PCs

All PCs should have anti-virus software installed on them. At very least, make sure you install a free anti-virus program such as AVG, Avast! or Microsoft Security Essentials (MSE). MSE is our absolute minimum recommendation for protecting your PC, but it's worth noting that, in recent tests in *Computer Shopper* magazine, it protected against only 80 per cent of viruses, compared with Kaspersky's 100 per cent protection.

It's generally worth buying paid-for anti-virus software because it usually comes with useful additional features. Not all paid-for anti-virus performs better than free software, but big-name products such as BitDefender and Norton Internet Security are generally reliable, although we've had issues with the performance of some of McAfee's products in the recent past.

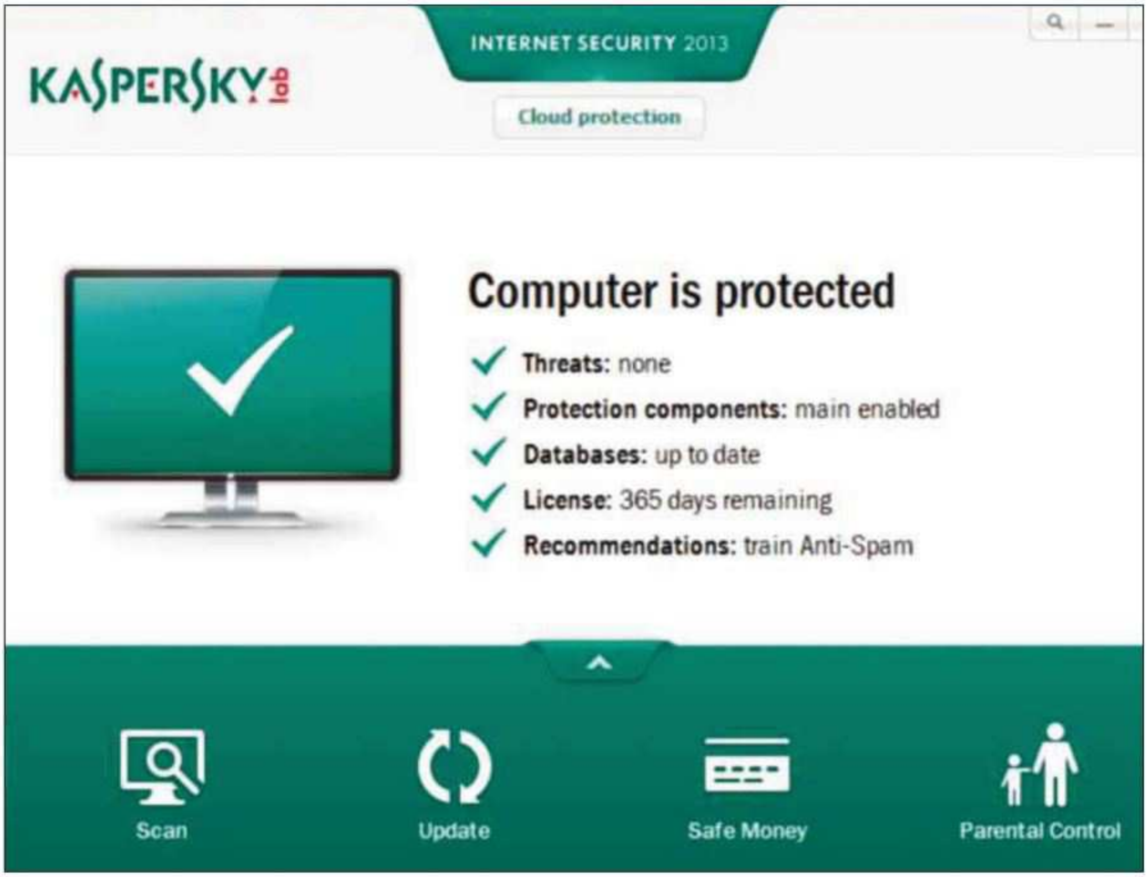
Computer Shopper's Best Buy winning anti-virus product this year is Kaspersky Internet Security 2013. You can get a three-PC licence for around £35 or a single-system licence for £20. It's simple to set up, allowing you simply to install it and then leave it to do its thing. It provides you with protection against malware from the web, within email and from instant-messaging clients, as well as the standard file scanning you can expect from more basic security products.

If you opt for free or basic paid-for anti-virus software, it will typically come with fewer features than most full internet security suites. However, other free programs are available to fill in the gaps.

WALL OF SOUND DEFENCE

Firewalls, whether hardware or software based, help to keep your system or (in the case of either dedicated hardware firewalls or the firewall built into your router) your network secure against unwanted network connections. Having a software firewall on your PC can help to protect it against malware on any local network to which you connect it.

> “Regardless of which security software you choose, it's also important to keep both your operating system and third-party software up to date.”



Computer is protected

- Threats: none
- Protection components: main enabled
- Databases: up to date
- License: 365 days remaining
- Recommendations: train Anti-Spam

In recent tests, Kaspersky Internet Security 2013 identified every single threat thrown at it

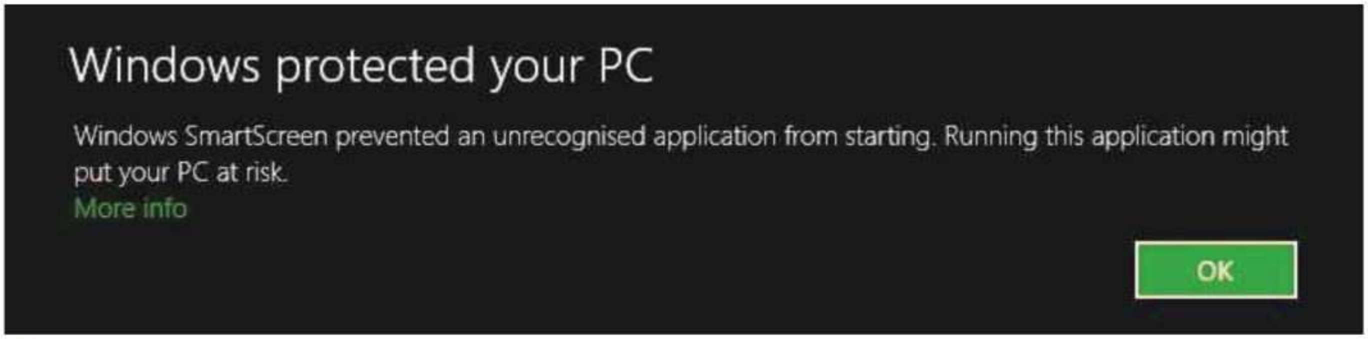
Since Windows 7, we've been entirely happy with Microsoft's integrated Windows Firewall, but if you prefer to use a third-party program, there are a number of popular free options, the best known of which is CheckPoint's ZoneAlarm Free Firewall (http://tinyurl.com/ZoneAlarmFirewall).

One of the most useful additional security applications you can install is a link scanner for your browser. These tools will alert you of potentially risky links in search results and, in some cases, on social media pages. AVG's Secure Search (www.avg.com/gb-en/secure-search) is among the most popular, marking potentially dangerous search results, blocking access to pages that AVG's web reputation engine has rated as dangerous and incorporating a Do Not Track feature that shows you what ad networks, social buttons and analytics engines are monitoring your browsing habits on any given sites. It's worth noting that link checkers can slow down your browsing, particularly on slower computers and internet connections.

Regardless of which security software you choose, it's also important to keep both your operating system and third-party software up to date. New security vulnerabilities – known as zero-day exploits when they are taken advantage of on the same day they're discovered – crop up on a daily basis, so best practice is to configure automatic update checking for all your critical applications. Unless you frequently use mobile broadband or a connection with similarly restrictive transfer limits, we recommend allowing your applications and operating system to update themselves automatically.

The software that's most frequently targeted includes web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera being the most common), Adobe's Reader and Flash and Oracle's Java. In general, the older and less frequently patched your operating system and software are, the more vulnerable they are . The deliberately vulnerable systems we use to test anti-virus software run Windows XP with Service Pack 3 and no further updates. If your own PC is running a similar software setup, it's time to run some updates.

> “A golden rule of operating system security is never to log in as administrator for day-to-day computing tasks.”



Windows protected your PC

Windows SmartScreen prevented an unrecognised application from starting. Running this application might put your PC at risk.

More info

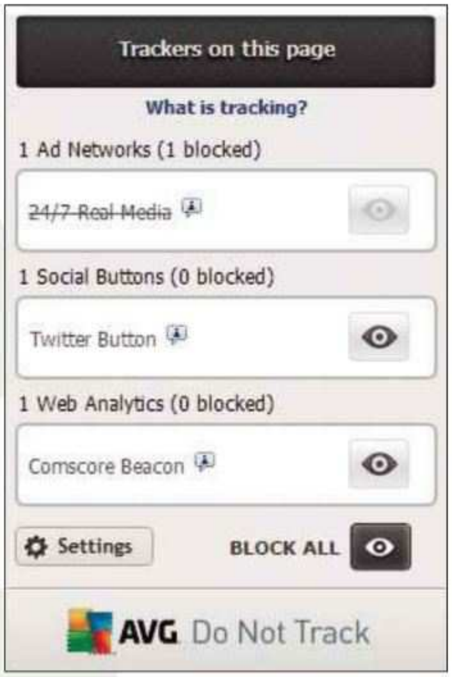
OK

Windows 8's SmartScreen tool automatically blocks the execution of any program it doesn't recognise

A golden rule of operating system security is never to log in as administrator for day-to-day computing tasks. Although it was common to do this under Windows XP, all modern operating systems go out of their way to encourage (or oblige) you to use user accounts. Options such as 'Run as administrator' under Windows and 'sudo' under Linux and Mac OS mean you can run applications with administrator privileges as and when you need them. If you're logged in as an administrator, any program run inherits the same admin access, so if you were to open a website containing malware, there'd be nothing to stop the malicious software from having full access to every system setting and command on your PC.

We also recommend leaving Windows' default User Account Control (UAC) settings enabled. This helps to prevent unwanted software from installing itself on your PC without your knowledge by asking permission whenever a program makes changes to the system. The minor annoyance of reading an extra pop-up is worth the ability to spot programs trying to install themselves without your knowledge.

Windows 8 adds its SmartScreen tool, which blocks the execution of any program it doesn't recognise. This will catch the vast majority of malicious executables, but it will occasionally block a little-known legitimate program. Fortunately, if you're sure the program you're trying to run is legitimate, you can simply click 'More info' and then 'Run' anyway. Similar features are implemented by many internet security suites.



Trackers on this page

What is tracking?

1 Ad Networks (1 blocked)

~~24/7 Real Media~~

1 Social Buttons (0 blocked)

Twitter Button

1 Web Analytics (0 blocked)

Comscore Beacon

Settings

BLOCK ALL

AVG Do Not Track

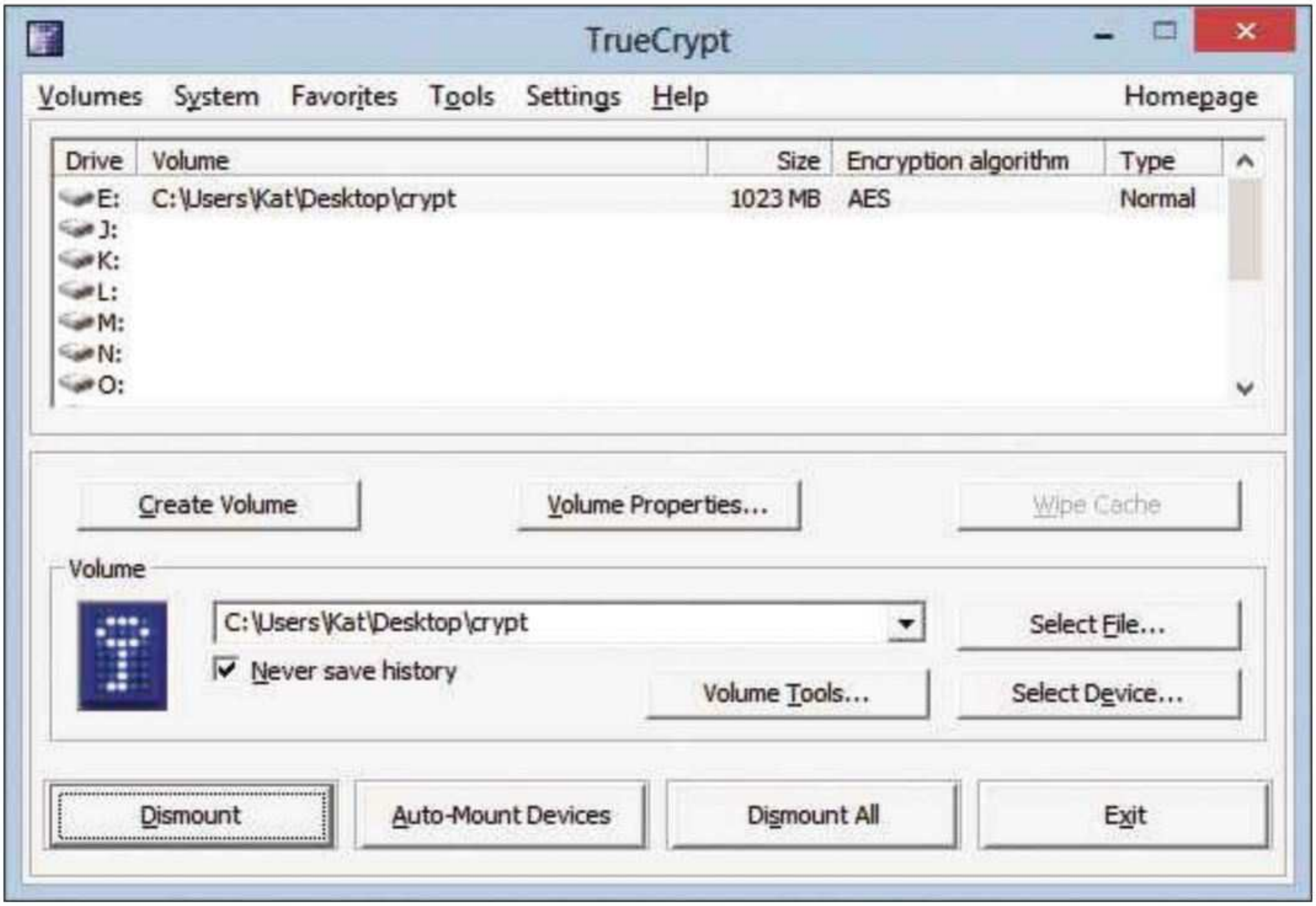
AVG's Secure Search tells you who or what is tracking your browsing habits

PASSWORD PROTECTION

Mac OS X and most Linux distributions insist that you set a password to log into your computer, while Windows strongly encourages you to do so. You should always set one, and choose one that is hard to guess. Avoid obvious choices such as 'password' or 'abcd1234'. Rather than using random strings of letters and numbers, it's often more secure to use a longer phrase, such as a quote from your favourite film, perhaps with a number substitution in it. 'Mynameis1nigomontoya' is not only memorable (if you're a *Princess Bride* fan, at any rate), but secure, too.

By setting a password, you make it more difficult for either thieves or someone who's gained access to your network to get on to your PC, where they could potentially access files or uninstall your security software. However, even if you have a password set, that doesn't necessarily protect your files if a thief has physical access to your computer, where they could then access your drives (and the files contained) using another operating system. To protect against this, see our guide to encryption *(opposite)*.

CYPHERSPACE: A QUICK GUIDE TO ENCRYPTION



Drive	Volume	Size	Encryption algorithm	Type
E:	C:\Users\Kat\Desktop\crypt	1023 MB	AES	Normal
J:				
K:				
L:				
M:				
N:				
O:				

Volume: C:\Users\Kat\Desktop\crypt

☑ Never save history

Once you've created your encryption file, TrueCrypt will mount it like a drive so you can use your file manager to drag anything you want protected into it

If you want to provide extra protection for the data on your hard disk, you can encrypt it. This ensures that, even if someone has physical access to your hard disk, they won't be able to read its contents unless they have your unique decryption key.

Our first choice for encryption is TrueCrypt (www.truecrypt.org), a free, open-source encryption tool for Windows, Linux and Mac OS X systems. You can use it to encrypt an entire internal or external hard disk, create a virtual encrypted disk or a special encryption file that acts like a folder you can use to store securely any files you don't want to leave in plain text on your hard disk, such as personal correspondence or financial records.

TrueCrypt is easy to set up: download and install it from the website, and after installation just follow the tutorial at http://tinyurl.com/TrueCryptTutorial.

Make sure you don't forget your decryption key, however, as you'll lose access to your encrypted data without it. It's unlikely to be an issue, but it's worth noting that UK law requires you to provide police with your cryptographic keys if presented with a warrant, with a penalty of up to two years' imprisonment if you don't do so.

Content filtering

Content filtering allows you to block access to specific kinds of material on the web, and is most often used to filter out adult websites. As well as its firewall and anti-virus components, Kaspersky Internet Security *(see page 88)* has a parental control module built into it. Other content-filtering software includes the well-known paid-for package CyberPatrol, and there are also free options such as BlueCoat's K9 Web Protection.

Most content-filtering software allows you to block websites and clean up search engine results based on keywords or subject matter. A number of content-filtering applications have additional features such as scheduling the times at which a specific user is allowed to access the internet, the ability to block certain programs and nude image detection (which is a brave effort, but typically imprecise at best).

Precision is an issue with many popular content-filtering applications. US programs in particular, including CyberSitter and CyberPatrol, have blocked sites belonging to human and civil rights groups, religious organisations and legitimate political parties. This extreme paranoia may be related to their use in US schools and public libraries, but it essentially means that the programs apply their makers' moral judgement to what your children should or shouldn't see, rather than necessarily reflecting your own views.

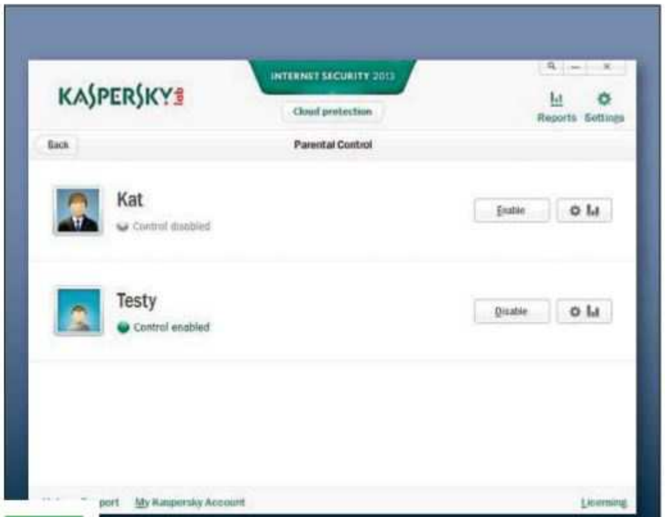
UK and European companies generally produce content-filtering applications more in tune with our own culture. However, in our tests we've encountered numerous parental control applications that have failed to block pro-anorexia and self-harm sites, while barring access to anti-drug sites and NHS sexual health advice for teenagers.

Content filtering isn't a substitute for sitting down and talking to your kids about what they might find online, and it won't take too much effort for a tech-savvy teenager to work their way around most parental controls. However, filtering of this sort is useful if you're trying to create a safe browsing environment for younger children.

> “Content filtering isn't a substitute for sitting down and talking to your kids about what they might find online.”

CONFIGURING KASPERSKY'S PARENTAL CONTROLS

Kaspersky's parental controls are quite thorough and are a free part of Internet Security 2013, our recommended anti-virus suite, so we'll take a look at its key capabilities and features. You're initially prompted to create a password to restrict unauthorised access to the parental control settings. Once you've set this up, you'll see a customisable icon representing each user on the PC.

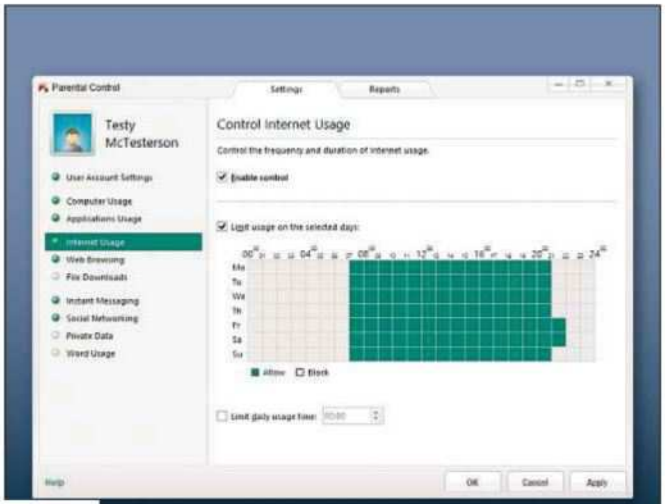


Kat – Control disabled

Testy – Control enabled

STEP 01

The main Parental Control screen provides access to both configuration data and usage reports for each user.



Control Internet Usage

Control the frequency and duration of internet usage.

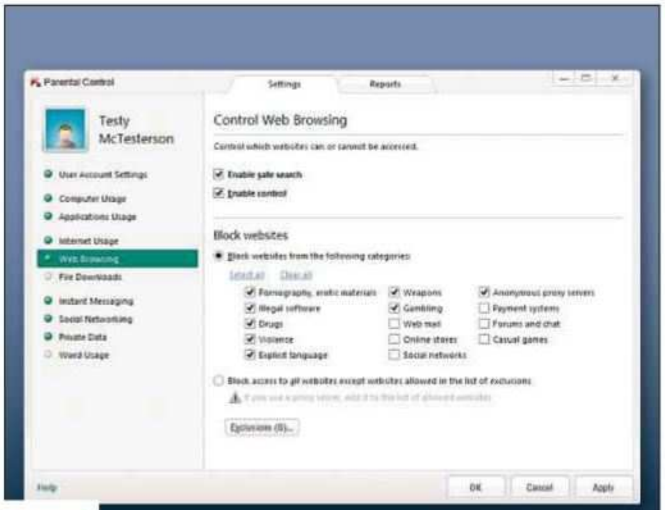
☑ Enable control

☑ Limit usage on the selected days:

☐ Limit daily usage time: 00:00

STEP 02

The Computer Usage, Internet Usage and Applications Usage tabs allow you to schedule the times at which a selected user is allowed to use the computer, go online or run specific programs.



Control Web Browsing

Control which websites can or cannot be accessed.

☑ Enable safe search

☑ Enable control

Block websites

● Block websites from the following categories:

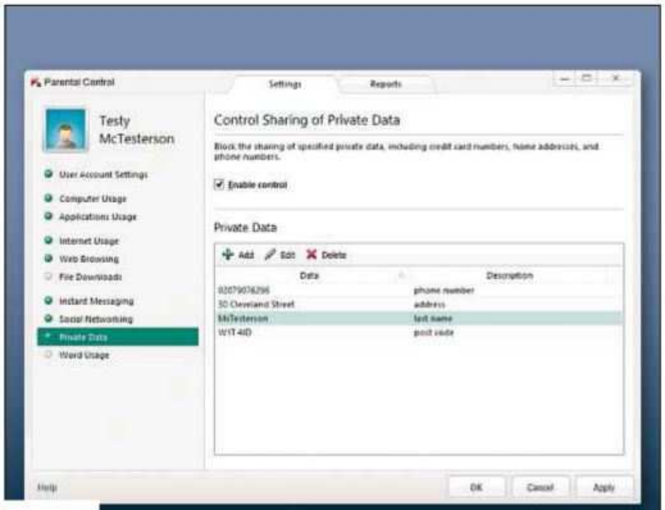
☑ Pornography, erotic materials ☑ Weapons ☑ Anonymous proxy servers
☑ Illegal software ☑ Gambling ☐ Payment systems
☑ Drugs ☐ Web mail ☐ Forums and chat
☑ Violence ☐ Online stores ☐ Casual games
☑ Explicit language ☐ Social networks

○ Block access to all websites except websites allowed in the list of exclusions

If you use a proxy server, add it to the list of allowed websites

STEP 03

The Web Browsing controls enable safe search modes and traditional parental controls, which restrict sites based on broad content categories that allow you to block everything from pornography and gambling to social networks and casual games. You can also add specified exclusions of your own.



Control Sharing of Private Data

Block the sharing of specified private data, including credit card numbers, home addresses, and phone numbers.

☑ Enable control

Private Data

Data	Description
02079076296	phone number
30 Cleveland Street	address
McTesterson	last name
W1T 4JD	post code

STEP 04

Private Data is particularly helpful. It prevents the user sending specified lines of data to a web page, chat client or similar. While this isn't an absolute way of ensuring your child can't give out their address – it could still be spelt out letter by letter, for example – it helps prevent them inadvertently sharing personal information or using your credit card number online.

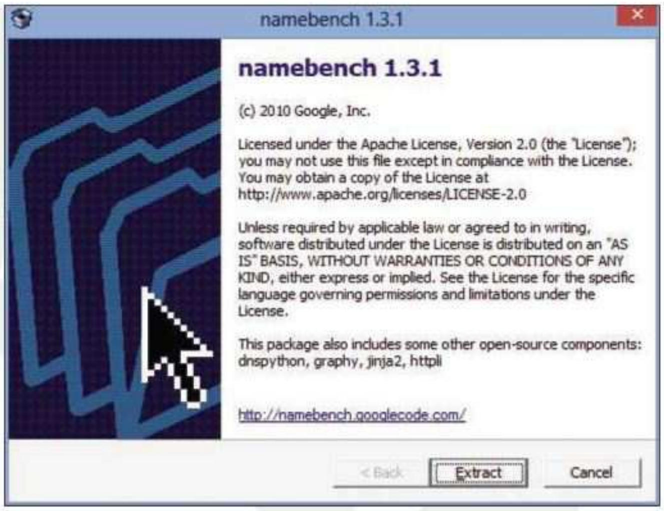
Speeding up web browsing with faster DNS

Everything connected to the internet has its own IP address, which is a string of numbers separated by dots. Humans are poor at remembering strings of numbers, which is why web addresses tend to consist of groups of words: www.bbc.co.uk is easier to remember than 212.58.244.67, for example. DNS servers are the computers that turn words into IP addresses and so make the web easy to use.

DNS servers are usually provided by your ISP and, if they take too long to respond to a request, it can slow your web browsing down significantly. Fortunately, there are alternative free DNS servers available, which can not only speed up your web browsing but also make surfing the web more secure. Over the next few pages, we'll show you how to test your current DNS server's performance, how to change to a different DNS server and how to take advantage of the advanced features a configurable DNS server can provide.

TESTING DNS

Which DNS servers are best for you depends on several factors, including your location and the websites you visit most often. To find the best match, you'll need to run some tests. Several programs that will do this for you. Our favourite is Namebench, as it's so easy to use.



namebench 1.3.1

namebench 1.3.1

(c) 2010 Google, Inc.

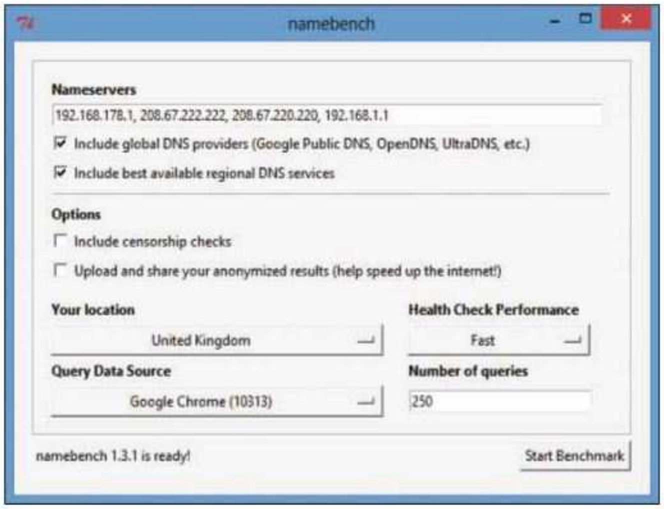
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This package also includes some other open-source components: dnspython, graphy, jinja2, httpli

http://namebench.googlecode.com/

You'll need to run the Namebench setup file every time you want to use it



namebench

Nameservers

192.168.178.1, 208.67.222.222, 208.67.220.220, 192.168.1.1

☑ Include global DNS providers (Google Public DNS, OpenDNS, UltraDNS, etc.)

☑ Include best available regional DNS services

Options

☐ Include censorship checks

☐ Upload and share your anonymized results (help speed up the internet!)

Your location: United Kingdom

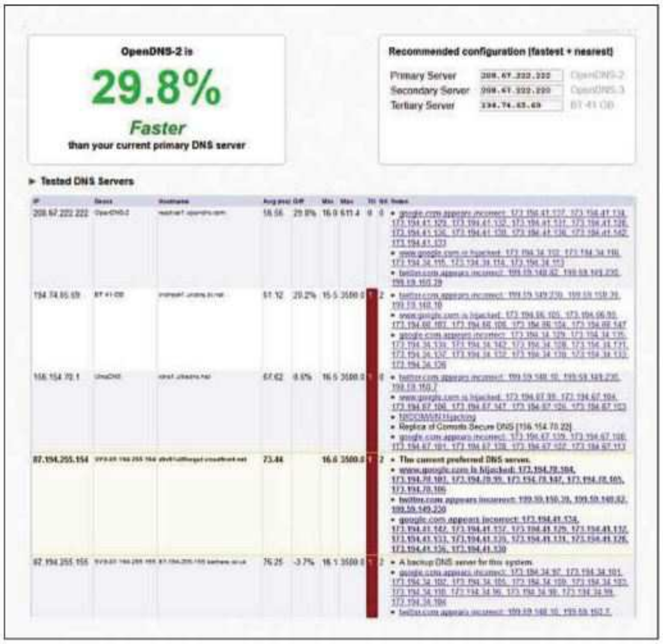
Health Check Performance: Fast

Query Data Source: Google Chrome (10313)

Number of queries: 250

namebench 1.3.1 is ready!

You should delete your router's IP from the Nameservers box for accurate results



OpenDNS-2 is

29.8%

Faster

than your current primary DNS server

Recommended configuration (fastest + nearest)

Primary Server	208.67.222.222	OpenDNS-2
Secondary Server	208.67.222.220	OpenDNS-3
Tertiary Server	194.74.65.69	BT-41-OB

► Tested DNS Servers

IP	Descr.	Hostname	Avg (ms)	Diff	Min	Max	TO	NX	Notes
208.67.222.222	OpenDNS-2	[illegible]	18.56	29.8%	16.0	611.4	0	0	• google.com appears incorrect: [illegible] • www.google.com is hijacked: [illegible] • twitter.com appears incorrect: [illegible]
194.74.65.69	BT-41-OB	[illegible]	51.12	29.2%	15.5	3500.0	[illegible]	2	• twitter.com appears incorrect: [illegible] • www.google.com is hijacked: [illegible] • google.com appears incorrect: [illegible]
156.154.70.1	UltraDNS	[illegible]	67.62	8.6%	16.5	3500.0	[illegible]	0	• twitter.com appears incorrect: [illegible] • www.google.com is hijacked: [illegible] • NXDOMAIN Hijacking • Replica of Comodo Secure DNS [156.154.70.22] • google.com appears incorrect: [illegible]
87.194.255.154	[illegible]	[illegible]	73.44		16.6	3500.0	[illegible]	2	• The current preferred DNS server. • www.google.com is hijacked: 173.194.78.104, [illegible] • twitter.com appears incorrect: 199.59.150.39, 199.59.148.82, 199.59.149.230 • google.com appears incorrect: 173.194.41.174, [illegible]
87.194.255.155	[illegible]	[illegible]	76.25	-3.7%	18.1	3500.0	[illegible]	2	• A backup DNS server for this system. • google.com appears incorrect: [illegible] • twitter.com appears incorrect: [illegible]

Namebench's results page shows you the speed of your current DNS servers and gives you a recommended DNS configuration

First of all, download Namebench from https://code.google.com/p/namebench. Double-click the downloaded file, and click Extract. The utility will extract itself to a temporary folder and run; it won't install itself in your Program Files folder or create a Start menu entry, so you'll need to extract it each time you want to use it.

The Namebench window has a number of options. The Nameservers box contains DNS servers that you definitely want to include in the search. This may contain the current IP address of your router (most likely in the format 192.168.xxx.xxx). Some routers cache DNS entries, so this will skew your results, as the router itself will always come out as the fastest DNS server. We recommend deleting such entries from the Nameservers box, as you will then see results for real DNS servers rather than your router's cache.

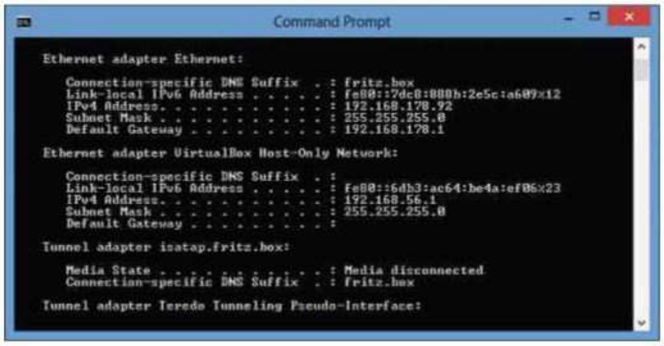
You should also leave the two options under the Nameservers box ticked. The first will give you results from popular third-party DNS services such as OpenDNS and Google's Public DNS, which is useful as these are the DNS servers to which you will most likely switch. The second box will return results for local DNS servers. You may not be able to use these, and we find they're rarely the fastest, but they make for an interesting comparison with your current ISP's DNS servers.

You can leave the other options at their default settings, but you may want to change the Query Data Source option. This uses your browser's history to record your browsing habits. If you have more than one browser installed, you can select a different browser from this list. You can also use a list of the top 2,000 websites, as measured by Alexa. This can be useful if you don't have many sites listed in your browsing history, but it isn't particularly personalised or accurate. According to Namebench's creator, many of those top 2,000 websites are in China, so are unlikely to be accessed very often by someone in the UK.

Click Start Benchmark to run the tests. This can take up to half an hour. When it's finished, the program will open your browser and display a summary of the tests. The main part you need to worry about is the box at the top that says which DNS server is the best for you. This may be your current server, but it's likely that a different server will provide you with better response times. Here we'll explain how to change your DNS server settings.

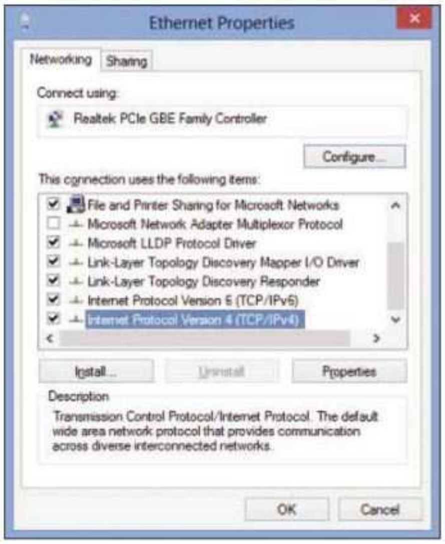
The report contains a wealth of information. If you're thinking primarily about speed, the Mean Response Duration bar graphs (halfway down) are the most useful, as they give you an at-a-glance breakdown of how various DNS servers perform. You can also look at the Response Distribution Charts to see whether most DNS queries have a similar response time, or whether a few very slow responses are dragging down the average.

The first page of the report shows a list of the servers tested. You'll see a mix of the global and local DNS servers, and a summary of response times. The Notes field can appear a little alarming at first. If a domain name is listed as 'hijacked' or 'incorrect', this shows when the DNS server returned a different IP address to what Namebench was expecting from a given web address. In extreme circumstances, this can mean that a DNS server is trying to redirect you for nefarious purposes, but the redirects we experienced seemed to be benign, such as www.google.com redirecting to www.google.co.uk and http://twitter.com to https://twitter.com.



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fritz.box
   Link-local IPv6 Address . . . . . : fe80::7dc8:888b:2e5c:a609%12
   IPv4 Address. . . . . . . . . . . : 192.168.178.92
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.178.1

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6db3:ac64:be4a:ef06%23
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.fritz.box:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : fritz.box

Tunnel adapter Teredo Tunneling Pseudo-Interface:
```

Running IPconfig from a Windows command prompt will show you the IP address of your router



Ethernet Properties

Networking | Sharing

Connect using:

Realtek PCIe GBE Family Controller

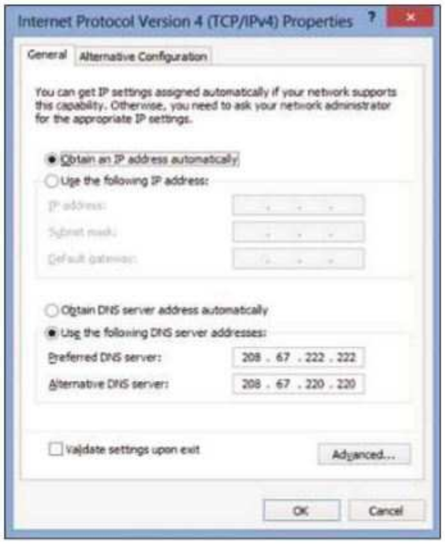
This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Open the Properties window for the network adaptor you use to connect to the internet...



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternative Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 208 . 67 . 222 . 222
Alternative DNS server: 208 . 67 . 220 . 220

☐ Validate settings upon exit

...and enter the address of the DNS servers you want to use to speed up your connection

SETTING YOUR DNS SERVERS

If you just want to have the fastest DNS server possible, you should use the configuration at the top-right of the Namebench report. This will give you a primary DNS server (usually the fastest), followed by a couple of recommended backups. You may even find that your ISP's DNS server is the fastest, so you don't even need to change anything. However, switching to OpenDNS will give you access to some powerful features that you won't get from your ISP's DNS server, so if there's not too much of a speed difference you may want to change servers anyway. We'll go into OpenDNS's extra features below.

The simplest way to enter the new DNS settings is from within Windows. Type Windows-R and type control netconnections to bring up your network connections box. Right-click on your network connection and click Properties, then double-click on Internet Protocol Version 4 (TCP/IPv4). Select the 'Use the following DNS server addresses radio' button, then enter the new DNS servers in the primary and secondary fields. Click OK and then open a website to make sure the new configuration is working properly. If there's a problem – such as the new DNS server not being publicly accessible, for example – try a different server or go back to the Internet Protocol Version 4 option and reselect the 'Obtain DNS server address automatically' option.

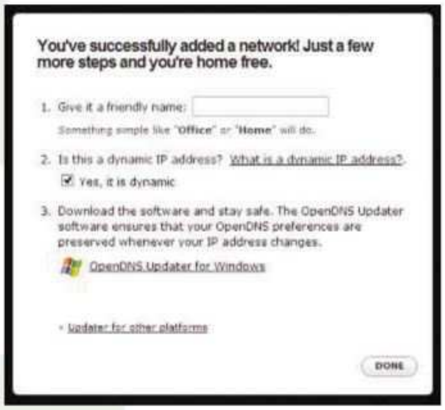
This is the simplest way of setting your DNS server, but the disadvantage is that you will have to enter the DNS server addresses manually on every computer on your network (and you won't be able to change the servers on smartphones or tablets).

To make sure that every device you have connects to the internet through your preferred DNS servers, you'll need to specify the DNS settings manually in your router's configuration pages. Unfortunately, not all routers allow you to do this, and the procedure will vary between models. You'll need to go into your router's setup page by typing its address into your web browser, then look for the home network section and IP address section.

To access your router's setup page, press Windows-R and type cmd to open a command prompt, then type ipconfig. Your router's address will be listed under Default Gateway. Type this into your web browser and enter the router's username and password; these are often both 'admin', or on a sticker on the bottom of the router or in the manual.

USING OPENDNS

A different DNS server may give you a speed boost, but the OpenDNS servers have another advantage in that they allow you to configure the DNS server, in order to block access to

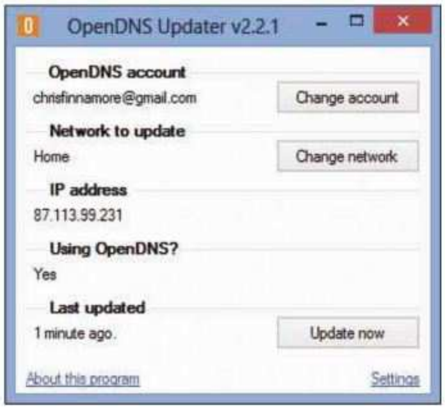


You've successfully added a network! Just a few more steps and you're home free.

1. Give it a friendly name:
   Something simple like "Office" or "Home" will do.
2. Is this a dynamic IP address? What is a dynamic IP address?
   ☑ Yes, it is dynamic
3. Download the software and stay safe. The OpenDNS Updater software ensures that your OpenDNS preferences are preserved whenever your IP address changes.
   OpenDNS Updater for Windows

- Updater for other platforms

Most home users will have a dynamic IP address, so should download the Updater client



OpenDNS Updater v2.2.1

OpenDNS account
chrisfinnamore@gmail.com

Network to update
Home

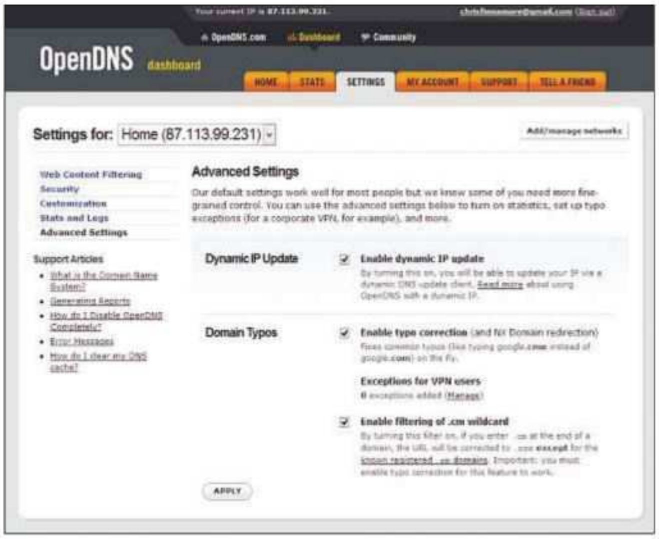
IP address
87.113.99.231

Using OpenDNS?
Yes

Last updated
1 minute ago.

The Updater client runs in the background and makes sure OpenDNS has your latest IP address

The OpenDNS dashboard has various settings to make your life online easier and safer



Settings for: Home (87.113.99.231)

Advanced Settings

Our default settings work well for most people but we know some of you need more fine-grained control. You can use the advanced settings below to turn on statistics, set up typo exceptions (for a corporate VPN, for example), and more.

Dynamic IP Update

☑ **Enable dynamic IP update**
By turning this on, you will be able to update your IP via a dynamic DNS update client. Read more about using OpenDNS with a dynamic IP.

Domain Typos

☑ **Enable typo correction** (and NX Domain redirection)
Fixes common typos (like typing google.cmo instead of google.com) on the fly.

Exceptions for VPN users
0 exceptions added (Manage)

☑ **Enable filtering of .cm wildcard**
By turning this filter on, if you enter .cm at the end of a domain, the URL will be corrected to .com **except** for the known registered .cm domains. Important: you must enable typo correction for this feature to work.

Support Articles

- What is the Domain Name System?
- Generating Reports
- How do I Disable OpenDNS Completely?
- Error Messages
- How do I clear my DNS cache?

unsuitable websites or to redirect you automatically to the correct website if you commonly mistype a certain address.

To get the most out of OpenDNS, you should use it with a router that lets you specify DNS addresses, so that your children can't get around parental controls by using a tablet or a phone to access the internet instead of the family PC. However, if those in your household only access the internet using PCs or laptops, you'll be fine setting it up in Windows.

You can set up OpenDNS by simply entering its servers (208.67.222.222 and 208.67.220.220) as your primary and secondary DNS servers, but to use its advanced features you'll need to create an account. Go to https://store.opendns.com/get/home-free and create an account with the form on the right. A confirmation email will be sent to the address you gave, so click the link to confirm your account. This will take you to the OpenDNS dashboard, which you can also access by typing dashboard.opendns.com in your browser. To add your network, click the 'Add a network' button on the Dashboard's Home section. Your external IP address (the address your router has on the internet) should already be listed, but if for some reason it's not there, simply type 'What's my IP' into Google to find it. Click the Add This Network button.

You'll now see a window asking you to give your network a friendly name, such as Home. It will also warn you about having a dynamic IP address. Most home broadband accounts have dynamic IP addresses, which means you occasionally receive a new external IP address from your internet service provider. We recommend downloading and installing the OpenDNS updater from this page, which will update OpenDNS automatically when you receive a new IP address. You only need to install the updater on one computer on your network, which should be the one that is used most often to make sure any IP address changes are picked up. Install the program and sign in with your OpenDNS username and password, then click the Add network button. It will now run in the background and keep OpenDNS updated.

Go back to the Settings section of the OpenDNS dashboard and select your network from the Settings for box to see the DNS settings you can tweak. The two sections we'll look at here are Advanced Settings and Web Content Filtering.

As you're running the IP address update client, you'll want to leave the 'Enable dynamic IP update' box ticked. The other useful option is Enable typo correction. This will take common typos such as www.google.cmo and direct you to the correct website rather than showing an error page.

The redirection will work fine in Internet Explorer and Firefox, but Chrome's Omnibox address bar will always search Google instead of redirecting to the correct place. It's a bit drastic to disable Omnibox searching just to be able to take advantage of the redirects, but it is possible.

In Chrome, open the menu at the top-right and click Settings. Click the Manage search engines box, and scroll to the bottom to find the three 'Add a new search engine' boxes. In the three boxes, from left to right, enter no, null and http://%s. Now click on the new search engine to select it and click the Make default button. This will create a dummy search engine for the Omnibox, and OpenDNS's redirects will now work.

PARENTAL CONTROLS

OpenDNS can also be extensively customised to filter out websites you don't want your family to see (or even yourself, if you're trying to go Facebook cold turkey). Presets range from High, which essentially blocks all social-networking sites and those to do with adult themes such as alcohol, to Low, which blocks only pornographic sites.

To see the categories blocked by each selection, click the View link. You can also manually select which categories are blocked within each preset by clicking the Customize link next to each one, so if you're fine with alcohol websites but not keen on your partner having access to dating sites, you can select the corresponding categories.

Even if you're not keen on blocking access to a particular kind of content, it's well worth selecting the Typo Squatting option. This will help stop you being redirected to those irritating 'What you want, when you need it'-style websites when you mistype a web address. Click Apply and wait a few minutes for the blocked sites list to propagate across OpenDNS's servers, and when you next try to go to a site from one of your selected categories, you'll see the OpenDNS block.

Securing your mobile devices

Your mobile phone is probably the most expensive item you carry around with you on a day-to-day basis. The police say that between 250,000 and 300,000 phones are reported stolen every year in the UK – and that's only the tip of the iceberg. Fortunately, there are steps you can take to protect your data and make it more likely that you'll see your phone again if it is lost or stolen.

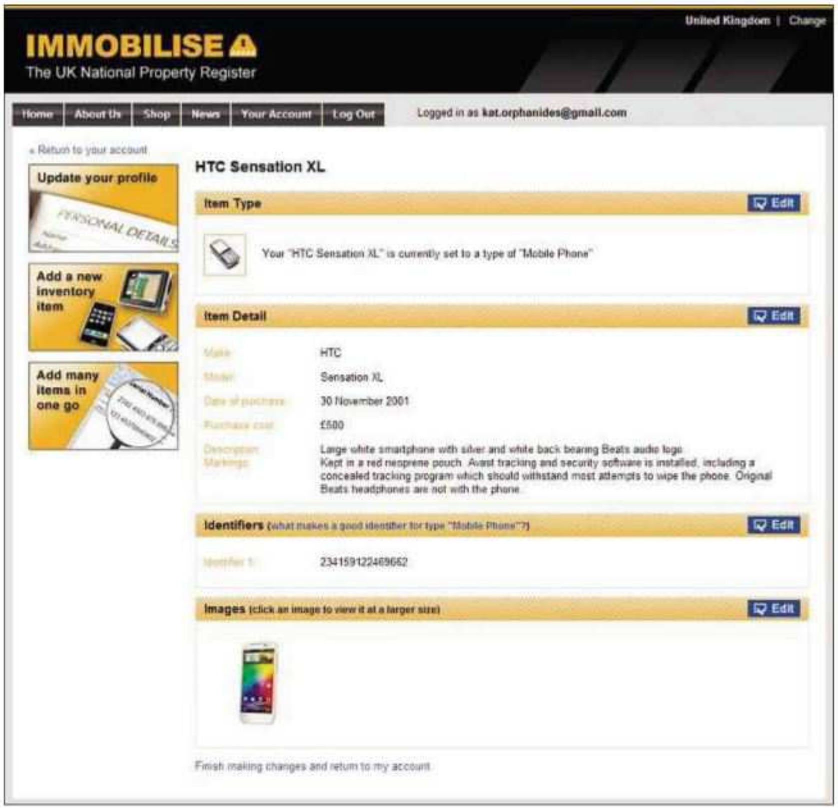
Your data is precious, so make sure that your phone is configured to back up your photos, videos and documents on a regular basis. Android users can use the Google+ app's Instant Upload feature to upload their photos to private cloud storage, while Apple's iCloud backup does the same for both photos and videos. There are also dedicated apps available for all phones, such as Sugarsync (www.sugarsync.com/products/sync_mobile.html) and Dropbox (www.dropbox.com/mobile), which will keep your content backed up in the cloud.

Keep all the information about your phone somewhere safe and easy to find should you need it. Most of the important documents, including proof of purchase, notification of your phone number and a record of the phone's IMEI, will be given to you as part of the bundle from your mobile provider if you get your phone as part of a pay-as-you-go or contract bundle. If you obtained your phone and contract separately, you'll have to pull all the bits together yourself.

Register your phone with Immobilise (www.immobilise.com). This free national property register allows you to notify police, insurers and second-hand retailers that your phone has been stolen straight away, making it harder for the thief to sell it on and more likely that it'll be detected when they try.

Mobile phone insurance can be an expensive business, particularly if you get it from your provider. Insurance for a top-of-the-range phone such as an iPhone 5 or Samsung Galaxy S3 will cost you £13 a month from Vodafone and £15 per month from Orange. Paying that for two years costs about half as much as the value of the phone. Fortunately, there are cheaper alternatives, which are worth considering if you're accident-prone or live in a blackspot for mobile-phone theft.

Most home insurance policies will give you cover for your mobile devices when you're out and about, although you may have to list them by name on your policy. If you'd rather not risk



IMMOBILISE
The UK National Property Register

United Kingdom | Change

Home | About Us | Shop | News | Your Account | Log Out

Logged in as kat.orphanides@gmail.com

« Return to your account

Update your profile

Add a new inventory item

Add many items in one go

HTC Sensation XL

Item Type Edit

Your "HTC Sensation XL" is currently set to a type of "Mobile Phone"

Item Detail Edit

Make	HTC
Model	Sensation XL
Date of purchase	30 November 2001
Purchase cost	£500
Description Markings	Large white smartphone with silver and white back bearing Beats audio logo Kept in a red neoprene pouch. Avast tracking and security software is installed, including a concealed tracking program which should withstand most attempts to wipe the phone. Original Beats headphones are not with the phone

Identifiers (what makes a good identifier for type "Mobile Phone"?) Edit

Identifier 1:	234159122469662

Images (click an image to view it at a larger size) Edit

Finish making changes and return to my account

Registering your mobile phone and other expensive equipment with the Immobilise national property register makes it easy to report a lost or stolen item to police, insurers and second-hand retailers

> “Mobile phone insurance can be expensive, particularly if you get it from your provider. Fortunately, there are cheaper alternatives.”

raising the cost of your home insurance just to make a claim for a phone, we recommend specialised third-party insurance. Insurance 2 Go (www.insurance2go.co.uk) and Protect Your Bubble (http://uk.protectyourbubble.com) offer cover against loss, theft or accidental damage to your phone for £7 a month.

TRACKING SOFTWARE

IOS

Apple iOS users should set up the Find My iPhone service (www.apple.com/uk/icloud/features/find-my-iphone.html) when they first set up their device. If you already have an iPhone, iPod or iPad and want to enable the feature, just to go the Settings screen, tap the iCloud tab and turn on Find my iPad.

Once it's enabled, you can use the Find My iPhone website (www.icloud.com/#find) to pinpoint remotely the current location of your device on a map. You can then remotely erase all the data on it and lock it while displaying a message requesting that anyone who finds it get in touch with you. It can even play a loud noise to help you locate your phone if you think you've just dropped it behind the sofa.

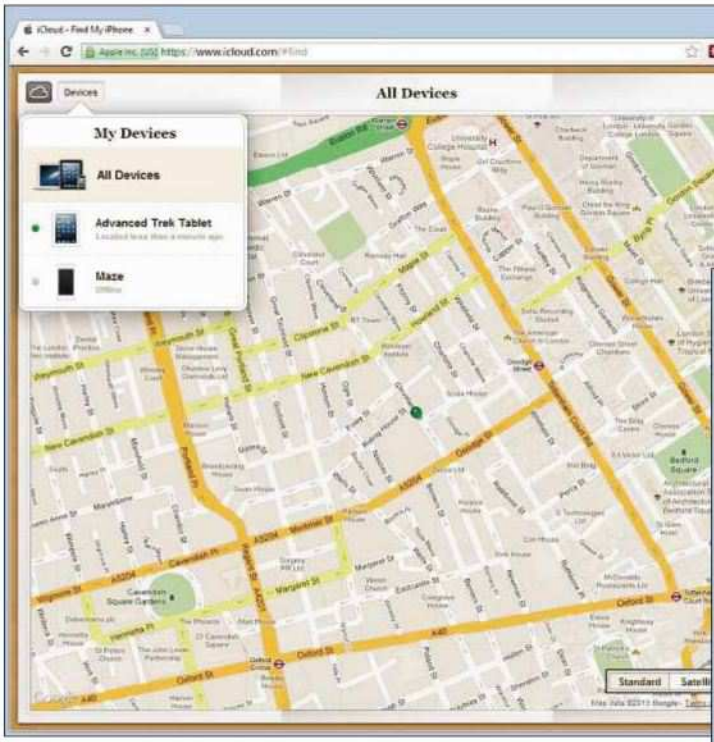
In its default state, Find My iPhone isn't particularly secure; there's nothing to prevent a thief from just turning it off in the Settings screen. However, if you go to the Restrictions screen on the General tab, you can set up your iOS device to require a passcode before anyone can make changes to its location settings. Simply press Enable Restrictions, then scroll down to the Location Services option under the Privacy settings. From here, you can select Don't Allow Changes to make it impossible to disable the Find My iPhone service without the passcode you set.

Regardless of what you do, Find My iPhone won't survive a full factory reset of your iOS device. Third-party tracking applications such as the free Prey Anti-Theft (http://tinyurl.com/PreyAntiTheft) won't do so either, but they can provide additional functionality such as the ability to take a photo remotely using the device's camera.

ANDROID

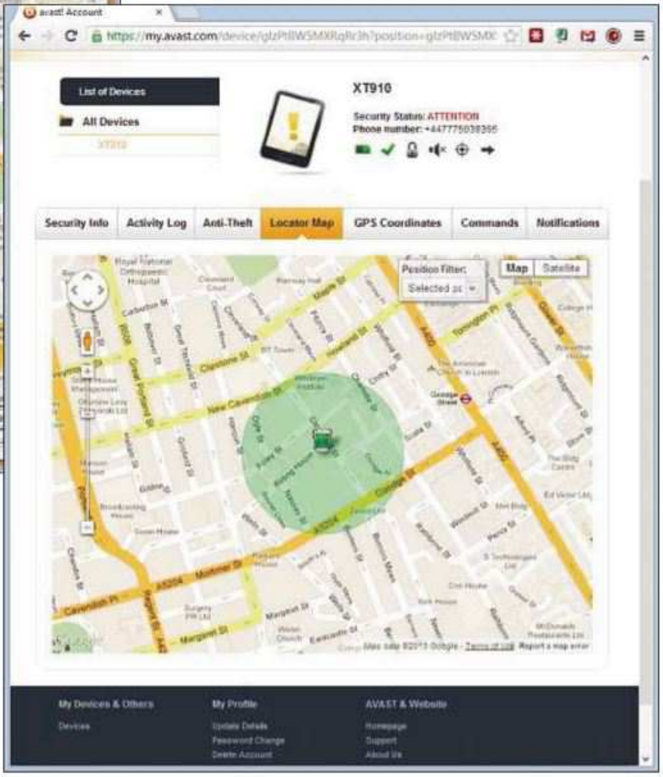
Android users can choose from a selection of location-tracking apps, some of which also include other security components such as anti-virus protection. Our favourite (not least because it located a stolen phone, which we were able to retrieve) is Avast! Anti-Theft, part of Avast! Free Mobile Security (www.avast.com/free-mobile-security). It's free, easy to conceal on your smartphone and can be made almost impossible to remove. Even without rooting our device to install the deepest level of security features, our phone survived an attempt by a thief to clear the phone, although it won't survive a full firmware wipe unless you root your device.

Once you've downloaded the package either from Google Play or directly from Avast! and installed it, you'll be prompted to set a security code and create an account so you can track, lock and wipe your phone via the http://my.avast.com website if it's lost or stolen. You can also send these commands to your phone via a text message – although you'll need to borrow a friend's phone to do so, of course.



It's easy to enable iOS's built-in location tracking, but you should take extra steps to prevent thieves from disabling it

Avast!'s web-based tracking interface makes it easy to get accurate location coordinates based on either GPS or Wi-Fi



Once it's installed and you've set a PIN, the application is essentially invisible; to access it, you have to enter the PIN on your phone's dialler. Configuring the app allows you to carry out tasks such as giving it system administrator permissions so that it can wipe your phone if necessary, but every step is clearly described, so you know exactly what's being set on your phone.

Some features, including the app's ability to switch on GPS tracking automatically when you send it a 'locate' command, don't work unless you've rooted the device. This limitation is common to Android anti-theft software due to the restrictions of the operating system, but we don't recommend rooting your phone unless it's out of warranty and you feel very confident about installing a rather fiddly array of third-party bootloaders.

Rooted or not, the app also warns you of potential security risks on your phone and provides protection against Android malware *(see box, opposite)*.

OTHER OPERATING SYSTEMS

Windows Phone users don't have many anti-theft apps to choose from, but Microsoft has integrated location tracking into the operating system itself. The Find My Phone services available via your www.windowsphone.com account allows you to make your phone ring and to lock, erase or locate it via your web browser.

None of the big names is available on BlackBerry devices, either, but the popular AntiTheft Free app (http://tinyurl.com/AntiTheftFree) has received positive feedback from users.

LAPTOPS

While there are now numerous tracking tools available for lost mobile phones, there's less talk about similar tools for laptops, despite the obvious risks of the loss or theft of a portable computer. Mac users can set up Apple's Find My Mac service, but you'll need to make sure your main OS X password is secure, as this is easily disabled by unticking the Find My Mac box in the iCloud menu under System Preferences.

For other computers, we recommend Prey (www.preyproject.com) an open-source cross-platform tool that can track a missing computer based on its IP address, GPS (if applicable) or local Wi-Fi hotspots. It can also grab a picture from a laptop's camera, see what your stolen computer is being used for in real time, lock down your data and remove stored passwords.

A free Prey account allows you to register only three devices of any kind of computer or mobile device. By default, Prey will report back every 25 minutes once you've notified the service that a device is missing, and the free account will

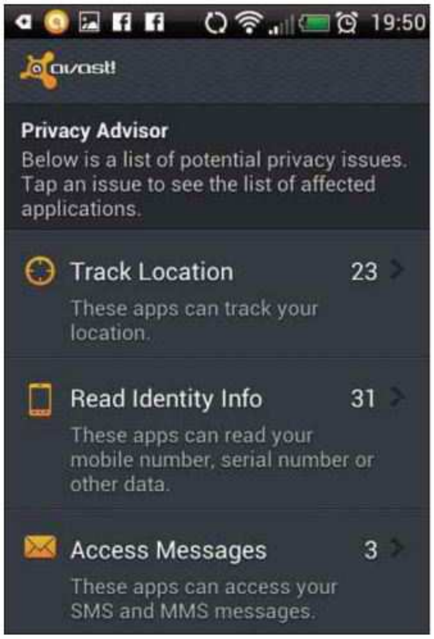
PLAY SAFE? ANDROID MALWARE

Malicious software targeting mobile phones and tablets represents a growing threat, with Google's Android operating system a favourite target. This is in part due to its popularity, and in part due to its inherent security vulnerabilities.

Unlike Apple's iOS devices, which allow users to install apps only from the company's own, rigorously secure, App Store, Android users need only tick a box to allow apps from any source to be installed. This is great for developers, early adopters, beta testers and even businesses that want to create custom apps in-house for their staff. However, it also opens the door to dubious third-party markets and bootleg software, which may come with an unexpected malicious payload.

Malware has also been repeatedly found on the official Google Play app store, despite Google's implementation of App Check malware scanning into Android 4.2 (Jelly Bean) and the increased security measures applied to apps that are submitted to the Play store.

Threats include apps designed to harvest your personal data, location and account passwords, malware designed to gain root privileges to your device, allowing malicious remote users to obtain full control of it, and SMS senders. These gain permission to use your phone's SMS feature and then send text messages to premium-rate numbers without your knowledge.



Privacy Advisor

Below is a list of potential privacy issues. Tap an issue to see the list of affected applications.

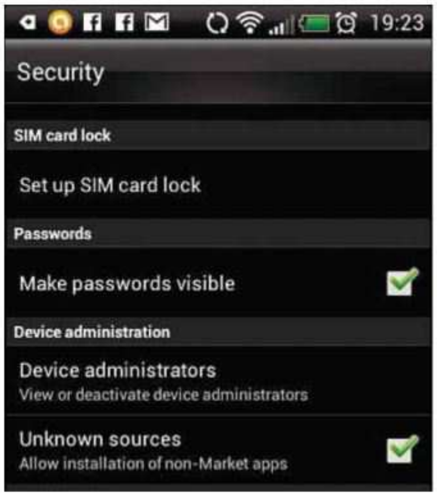
Track Location 23
These apps can track your location.

Read Identity Info 31
These apps can read your mobile number, serial number or other data.

Access Messages 3
These apps can access your SMS and MMS messages.

Avast! Free Mobile Security lets you monitor apps and websites for potential threats

No-one's going to install an app labelled 'Secret Premium Rate SMS Sender'. Whatever threat a malicious app presents, it will be cleverly disguised to make it appealing to its potential victims. It usually takes the form of a functional program that has been packaged with hidden capabilities. You'll be able to use the app itself normally to do whatever it's supposed to, but in the background it will be up to something far more unpleasant.



Security

SIM card lock

Set up SIM card lock

Passwords

Make passwords visible ☑

Device administration

Device administrators
View or deactivate device administrators

Unknown sources ☑
Allow installation of non-Market apps

Android users can allow apps from any source to be installed

While avoiding third-party app stores and not giving the phone permission to install apps from unknown sources are obvious precautions, the potential presence of malware within Google Play itself means that you should install additional security software.

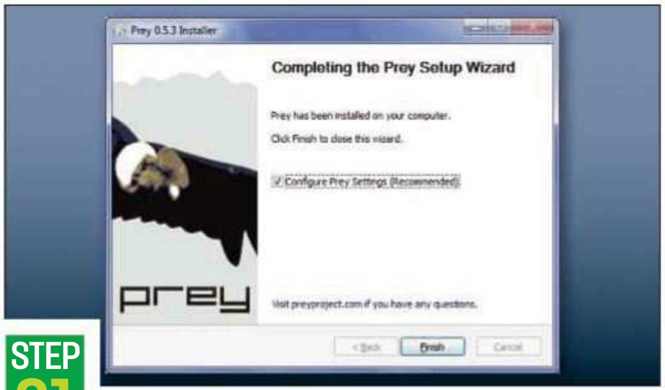
We recommend Avast! Free Mobile Security (www.avast.com/free-mobile-security), which provides tracking for lost or stolen Android devices. As well as scanning all APK files before they're installed, Avast! keeps tabs on what rights each program has, so you can see at a glance which apps can read your phone's identity information, track your location or access your messages. Other components include SD card scanning, monitoring of your browser and email for malware and phishing sites and even blocking incoming communications from unwanted numbers.

store only the last 10 reports for each device, so the eleventh report will delete the first.

A Prey Pro account (from $5 a month) stores up to 100 reports, among other useful extras. These reports can be configured to include screenshots, lists of local Wi-Fi hotspots, details of the IP address from which the stolen system is connected and as much geolocation data as the computer can glean from Wi-Fi or – if it has it – GPS. The program is hidden on your device, so you won't be able to see it once it's been installed, but then nor will anyone who's stolen your laptop. Because of this, you use a web interface to change settings.

Regardless of which software you use to protect your computer against theft, you should have a strong password on every account on the system, especially accounts with administrator privileges. If a thief can't log in to your computer, they won't be able to start disabling your anti-theft software.

How to track a stolen laptop



Prey 0.5.3 Installer

Completing the Prey Setup Wizard

Prey has been installed on your computer.

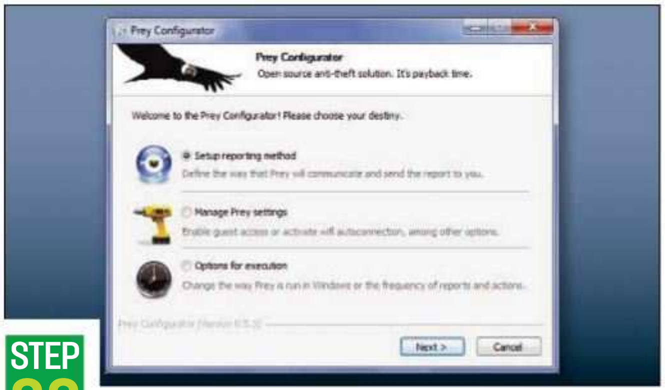
Click Finish to close this wizard.

☑ Configure Prey Settings (Recommended)

Visit preyproject.com if you have any questions.

STEP 01

On the computer you want to protect, go to http://preyproject.com and click on the green 'Free download' button. When the download is complete, find the downloaded file in Windows Explorer and double-click on it to start the installation. Follow the installation wizard until you get to the 'Completing the Prey Setup Wizard' dialog box. Make sure that 'Configure Prey Settings (recommended)' is selected before clicking the Finish button.



Prey Configurator

Prey Configurator
Open source anti-theft solution. It's payback time.

Welcome to the Prey Configurator! Please choose your destiny.

● Setup reporting method
Define the way that Prey will communicate and send the report to you.

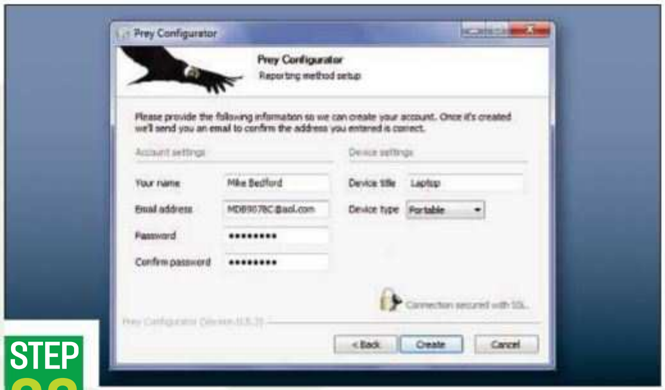
○ Manage Prey settings
Enable guest access or activate wifi autoconnection, among other options.

○ Options for execution
Change the way Prey is run in Windows or the frequency of reports and actions.

Prey Configurator (Version 0.5.3)

STEP 02

You'll now see a warning message telling you that, since this is the first time you've run the program, you must set up your reporting method. Click OK and the Prey Configurator will appear. Select 'Setup reporting method' and click Next. The best option is 'Prey + Control Panel (recommended)', so select this and click Next.



Prey Configurator

Prey Configurator
Reporting method setup

Please provide the following information so we can create your account. Once it's created we'll send you an email to confirm the address you entered is correct.

Account settings

Your name: Mike Bedford
Email address: MD89078C@aol.com
Password: ••••••••
Confirm password: ••••••••

Device settings

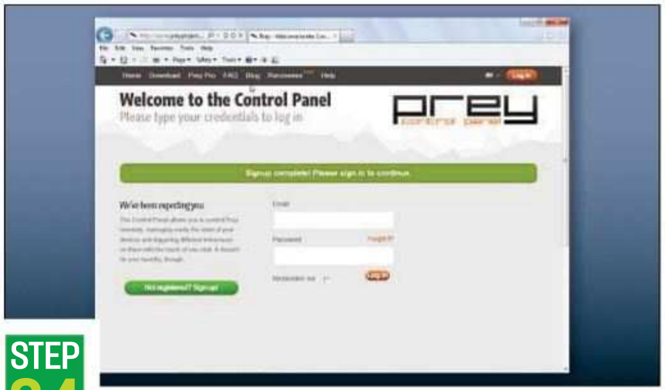
Device title: Laptop
Device type: Portable

Connection secured with SSL.

Prey Configurator (Version 0.5.3)

STEP 03

You'll be asked whether you've already registered for a Control Panel account at Preyproject.com. Assuming that you are new to Prey, select New user and click Next. Enter your name, email address, a password (twice) and a name for the device you're protecting, and select the type of device from the pull-down menu. Now click on Create to send a request to Prey.



Welcome to the Control Panel
Please type your credentials to log in

Signup complete! Please sign in to continue.

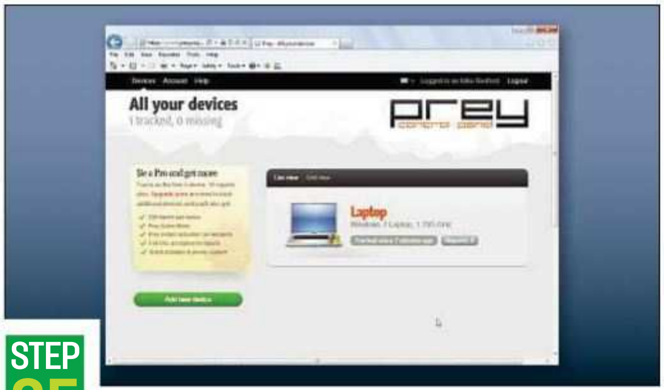
We've been expecting you

STEP 04

Look in your email inbox for a message from Prey. If you don't see it, it may be in your Spam folder. If so, the messages from Prey in Steps 6 and 7 will probably have the same fate. If the message contains an active link, click on it; if not, copy and paste it from the email into the address bar of your browser. You'll be taken to a page on the Prey website where you can log in using the email address and password that you gave in Step 3. Once you've logged on you'll see the opening page of the Prey Control Panel that you'll see each time you log on in the future.

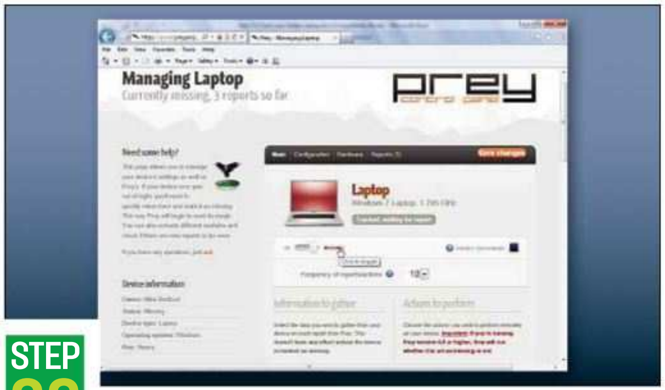
A stolen or lost laptop doesn't mean it's gone forever. In this walkthrough we'll show you how to keep tabs on a missing computer using the free Prey software, which will track a stolen laptop, so you can tell the police where it is.

As well as tracking your laptop, Prey lets you take photos with your laptop's webcam so you can see who's using it, and take screen grabs so you can see what they're up to. With the ability to lock your computer and delete files too, you can make sure your data is safe even if you can't retrieve your computer.



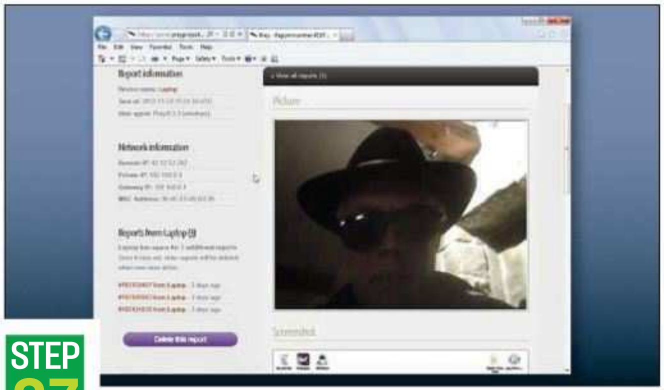
STEP 05

The first page of the Prey Control Panel lists all your protected devices. Click on the icon for the laptop you want to configure, which will have a blue screen (a red screen means you've reported it as missing). This will take you to the Control Panel for that device. Click the Main tab. The section 'Information to gather' specifies what information will appear in the reports that are generated if your laptop is reported as missing. The defaults are probably fine for now, but if you do change any, be sure to click on 'Save changes' when you're done.



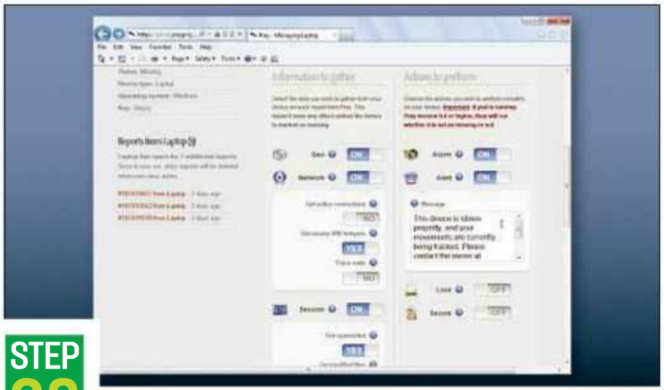
STEP 06

Go to http://panel.preyproject.com and log in. Here you can alter the settings, but it's also where you'll head to in the event of a theft. If you do discover your laptop is missing, go to the page for that device and, on the Main tab, click on the slider to change its status from OK to Missing, then select 'Save changes'. The 'Device information' section will be updated to show the device as missing and you'll receive an email confirming that and telling you when the first report will be available. You might also want to change the interval at which you'll receive reports.



STEP 07

You'll now get an email with a link to a report or, if you're still logged in to the Prey Control Panel, you'll see the report listed below 'Device information' at the left of the screen in the Main tab for the stolen device. Click on the orange link to view the report. This should include the various types of information that you accepted or altered in Step 5, ideally including a location map, a photo of whoever's using your PC and a screenshot. You may have to wait for a few reports before getting a proper photograph.



STEP 08

There comes a time, if monitoring hasn't been able to track down your laptop, to be more proactive. While logged into the Prey Control Panel and with the stolen device selected, go to the Main tab and you'll see a section entitled 'Actions to perform'. This provides you with several options, such as sounding an alarm or displaying a message of your choice on the stolen computer. You can also lock the laptop or hide sensitive information. In each case, click on the appropriate button(s) and then click on 'Save changes'.

Recovery position

Essential rescue guides

It's all very well knowing how to protect yourself against malware, fraud and theft, but what if the worst has already happened? Don't worry, help is at hand: you can use our handy guides to help you recover from the consequences of common security failures.

LOST OR STOLEN PHONE

Losing a phone or smartphone is a disaster for most of us. The loss of an expensive device is compounded by the potential responsibility for any bills incurred by the thief; added to which, of course, is the loss of your personal data and the inability to communicate with friends and family. Bear in mind that the police do not recommend dealing with potential thieves yourself.

01 If you're not certain whether your phone has been stolen or has simply been misplaced, it's worth phoning it from another phone. If your phone is set to silent mode, most phone security software can make a loud noise that will help you find it if it's nearby.

02 If it's definitely been stolen, report it to the police as soon as possible. They will provide you with an incident number that you'll need when making a claim with your insurance provider. If the incident is ongoing (if, for example, you've just had your bag snatched and you can see the robber pegging it down the road), dial 999. In other situations, where the crime has already occurred, call 101 or use your local police service's online crime reporting form. When reporting a crime after the fact, have your phone's IMEI number to hand. Remember to make a copy of the information you've entered into the online incident report form before submitting it.

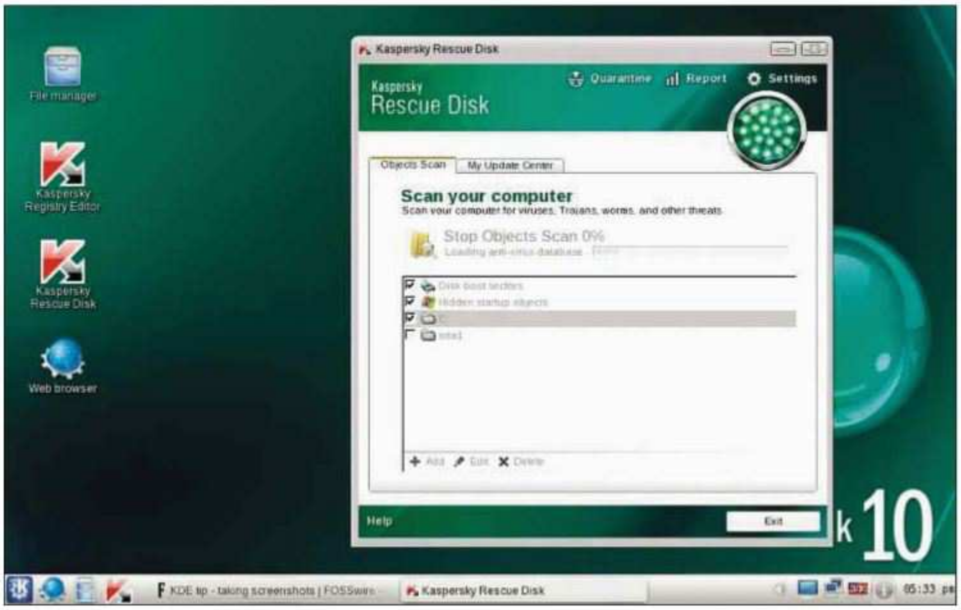
03 If you have tracking software installed on the phone, it's possible that you or the police officer dealing with your case will be able to use this to locate your missing device. If you suspect the phone has been lost, rather than stolen, you can use most tracking tools to lock the phone and display a message containing your contact details and any information about a finder's fee, use local GPS and Wi-Fi signals to tell you where it is, or have it phone you so you can try to work out where you lost it.

If your battery has run out, many tracking apps can be set to notify you when your phone is next switched on or if someone attempts to put a new SIM in it. If you don't already have tracking software installed, you could attempt the remote installation of an emergency tracking app such as Plan B for Android (http://tinyurl.com/PlanBAndroid). Apple's iOS apps can't be installed remotely.

04 Next, you should visit the Immobilise property register (www.immobilise.com) to list the phone in the national stolen property database for police forces and second-hand dealers. Contact your mobile phone provider to have them bar your SIM, which prevents calls being made from it, and block your phone's unique IMEI identification number. This block can later be reversed by your provider if you get your phone back, but will prevent it from being used in the interim.

Make a record of exactly when you called your mobile phone provider, in case they fail to block the phone correctly. It's important to block your phone as soon as you possibly can, as most insurance providers will cover you for calls made on a stolen phone only for 24 hours after its theft. Blocking your phone will also disable any tracking software you have installed on it.

05 Change any passwords that were saved on the device. This includes your Apple or Google password, as well as those for any third-party email providers, social media sites, online storage services and so on. If you had any banking passwords or PINs stored on the phone, change



Kaspersky's Rescue Disk is a bootable Linux distribution that you can use to scan your hard disk for malware or even copy over vital files from a compromised PC

those, too. Protecting yourself from identity theft and fraud is more important than the loss of any individual device and should be your main priority.

06 Before contacting your insurance company, you'll need your crime number. It's also advisable to have a copy of the report you gave to the police, which they should be able to provide to you. If your device isn't listed individually with your insurer, you'll probably need to have your proof of purchase to hand as well. Failing that, other proof of ownership, such as photos of the device in your possession, may help.

The more information you can provide to support your claim, the better. If you're claiming on your home insurance policy, check your excess and no-claims bonus against the cost of replacing the phone, as it may not be worth making a claim. Remember that making an insurance claim may increase your future premiums.

LOST OR STOLEN LAPTOP

Locating a missing laptop is a little different to locating a phone, but many of the key steps are the same. Once again, note that the police do not recommend dealing with potential thieves yourself. It's also illegal to buy back goods that were stolen from you – yours or not, it's handling stolen goods.

01 Report the theft to the police as soon as possible and note down the incident number. You'll need this in future dealings with both police and your insurer. Only call 999 if the crime is in progress; otherwise call 101 or use an online crime reporting form.

You'll need to provide as much detail about your laptop as possible. If you know the unique MAC address of your laptop's network adaptor, provide it. Make a copy of the information you've entered before submitting it in an online incident report.

02 List your computer on the Immobilise property register (www.immobilise.com), the national stolen property database for police forces and second-hand dealers.

> "If you don't already have tracking software installed, you could attempt the remote installation of an emergency tracking app."

03 If you have tracking software installed on your laptop, it's possible that you or the police officer dealing with your case will be able to use this to locate your missing device. If you suspect the computer has been lost, rather than stolen, tools such as Prey *(see page 102)* allow you to lock it and display a message containing your contact details.

04 If you have remote login software such as LogMeIn or GoToMyPC installed, you may be able to connect to your PC remotely. LogMeIn can even be used to wake a computer from sleep mode.

If you can connect to the computer, you can find out its IP address, which may help locate it. Online backup and synchronisation services such as Dropbox can also report the IP address from which your laptop last connected if you've installed the company's desktop client. Taking control of a missing PC is likely to alert a thief immediately that you're on to them, making them more likely to dump or trash your laptop, so it's best to do this only under police supervision.

05 Change any passwords that were saved on your PC, particularly anything that you may have had noted down in a file or saved in the web browser. This could be a very long list, including email and social-networking passwords. If there's any chance at all that you'd stored banking information on the computer, inform your bank.

06 When you speak to your insurer, you'll need a crime number and ideally a copy of the police report. If the laptop isn't individually listed with your insurer, you'll probably also need proof of purchase or other proof of ownership. If you're claiming on home insurance, check your no-claims bonus against the cost of a replacement laptop, as most PCs devalue quickly over the course of just a couple of years. Making a claim may raise the cost of future premiums.

THERE'S A VIRUS ON MY PC!

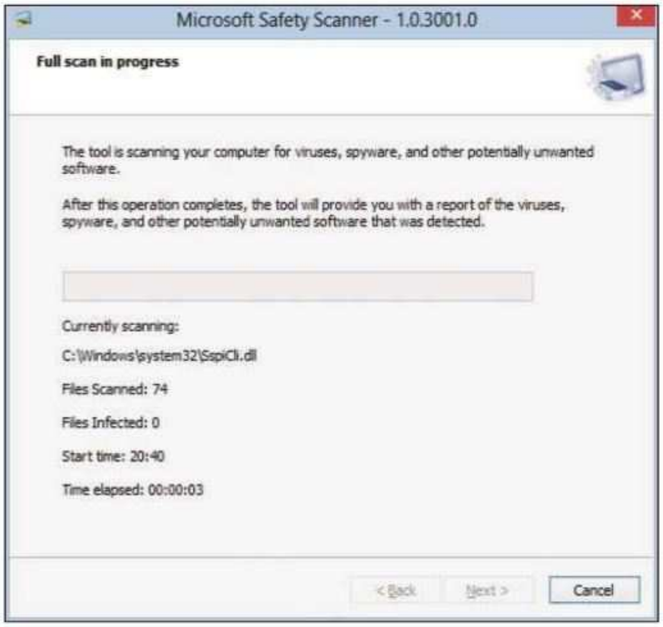
01 Don't panic. If your system is running slowly, crashing or behaving oddly, there are a number of potential causes, of which malware is only one possibility.

If you already have anti-virus software installed, run a full scan. If your system is unstable, boot into Safe mode before scanning, as this may prevent malware from interfering or doing further damage. Disconnect the potentially infected system from your network to keep it from transmitting malware to other systems and to prevent the malware from downloading further threats from a remote location.

02 Run Windows Update. Microsoft provides regular security updates that close routinely discovered vulnerabilities. You should also download and run the Microsoft Safety Scanner, which is available for free from http://tinyurl.com/MSSafetyScanner.

03 If you don't have anti-virus software, install and run a reputable program. Unfortunately, you will need to be online to download the software and the signature updates it will need to check your PC.

We recommend Kaspersky Internet Security 2013 (a single-PC licence costs £40 from www.kaspersky.co.uk). If you can't afford that, AVG Free (http://free.avg.com) is a good alternative. Remember not to install multiple anti-virus programs alongside one another. A notable exception to this is Malwarebytes (www.malwarebytes.org), the free version of which happily coexists with most other anti-virus software.



Microsoft Safety Scanner - 1.0.3001.0

Full scan in progress

The tool is scanning your computer for viruses, spyware, and other potentially unwanted software.

After this operation completes, the tool will provide you with a report of the viruses, spyware, and other potentially unwanted software that was detected.

Currently scanning:
C:\Windows\system32\SspiCli.dll

Files Scanned: 74

Files Infected: 0

Start time: 20:40

Time elapsed: 00:00:03

Microsoft's free security scanner quickly checks your system for the latest threats

Online virus scanners are also available, including BitDefender QuickScan (http://quickscan.bitdefender.com), which scans your entire PC, and Metascan (www.metascan-online.com), which runs an individual suspicious file through multiple scanning engines. Although these and other online scanners can't remove malware, they can tell you if you've got a problem on your hands.

04 If the malware is preventing you from booting Windows or running anti-virus software, you'll need to boot from something else. The simplest option is to download a bootable anti-virus rescue disc such as Kaspersky Rescue Disk 10 (https://support.kaspersky.com/viruses/rescuedisk). If you've installed Kaspersky Internet Security, you can create a rescue disc using its built-in tools.

05 Unfortunately, sometimes even rescue discs are unable to repair the damage done to your operating system. If it becomes clear that this is the case, it's often easier and less stressful to copy your vital personal data, media and images to an external drive using a bootable Linux distribution – such as Kaspersky's Rescue Disk – before reinstalling Windows from scratch.

Safeguarding your internet accounts

Google hates passwords, and it's not hard to see why. Strong passwords are tricky to remember, so people use weak ones instead. Then they use the same weak passwords for different services. The average internet user has dozens of online accounts that are secured with flimsy combinations of the same username and a couple of passwords, and this can turn a security problem into a full digital disaster.

Hacking attacks on well-known services are increasingly common. In 2012, file storage service Dropbox suffered an embarrassing breach, while in 2011 Sony's PlayStation Network service was down for 24 days and 77 million account details were stolen. Twitter was hacked as recently as January 2013, while individual Twitter accounts continue to be compromised regularly. No matter how large and respectable a service is, hackers are not only willing to attack it but are succeeding, too.

There's nothing you can do to stop hackers attacking services you rely on, but you can make sure that any leaks don't cascade across multiple services. Here we'll show you how to do this as effectively as possible, and how to regain control of your account if the worst happens. We'll also show you how to take basic steps to prevent more targeted attacks against you.

Google is looking at other ways to secure your online accounts, some of which are available already, while others will appear over the next few years. Google vice-president of security Eric Grosse recently stated: "Along with many in the industry, we feel passwords and simple bearer tokens such as cookies are no longer sufficient to keep users safe." It wants us to use more than a string of numbers and letters to authenticate our access to web accounts.

A first step is Google's support for two-step verification, where you must authenticate access from a new piece of hardware using a one-off code that's sent as a text to your phone. This has long been offered to Facebook, online-gaming service Steam and Google account users and had just been rolled out for Twitter as we went to press. It's a little awkward to set up if you use a lot of devices, but we think it has become essential. We'll discuss this in more detail later on.

Tiny, sturdy and simple to use, the YubiKey could mean the end of passwords for many of us

It's not only Google that's finally admitting that people are struggling to secure and manage their online accounts using the tools provided. PayPal and Twitter recently announced they would move in a similar direction, and Dropbox has embraced extra levels of security for its users in the past few months.

PAST-WORD

Looking further into the future, passwords will become less important. With a wave of a hand, the blink of an eye and possibly a quick punch of a PIN, you will be able to access your computer and internet accounts more securely and with more convenience than ever before. USB keys, NFC-equipped devices and even retina scanners look to be the future of online security, probably in combination with a simple PIN. This will make accessing your Gmail account very similar to taking out money at a cashpoint.

One possible solution that already exists is Yubico's YubiKey. Slot it into a spare USB port and it unlocks your email account at a touch. Your PC recognises the device as a keyboard, so no drivers are required, although the service must support YubiKey for it to work. A USB key would work with PCs, but a better option for smartphones would be a passive RFID chip (like those in Transport for London's Oyster cards) embedded in a ring that unlocks your smartphone when you pick it up.

This technology is available today, so it's simply a matter of the big services integrating it into their products. To make it successful, they'd have to give these security devices to users, which could be a problem for huge, free services with a global reach, such as Google's.

A largely password-free future may be just around the corner but it's certainly not here yet, so we're going to look at the options available and demonstrate how to secure your online accounts in more practical ways. If you've already been hacked, just follow our advice and you'll be able to take back control of your accounts and prevent similar problems in future.

TWO-STEP PROCESS

Google

2-step verification
https://www.google.com/settings/security

facebook

Login approvals
https://www.facebook.com/settings?tab-security

twitter

Account security
https://twitter.com/settings/account

Microsoft

Two-step verification
https://account.live.com/proofs/Manage

Dropbox

Two-step verification
https://www.dropbox.com/account#security

amazon

Only available for web-hosting services

HOW DO THEY HACK?

Before we look in detail at how you lock down your accounts, it's useful to understand how the bad guys try to gain access. If you know the weak points in the security systems you use, you'll better understand how to improve your own security.

One option available to the criminals is to steal your username and password from you directly. They might use malware to extract the information from your computer, trick you into handing them over using phishing emails or pull the data off the network as you log in, perhaps over a wireless network. Alternatively, they might trick online services into handing over your information, launch a technical attack against the company or simply buy your data from someone who has already stolen it using any of the above methods.

These are the main approaches that criminals take, and while we won't dig too deeply into exactly how they work and how their underground economy is organised, it's useful to know what you can protect yourself against and how.

PROTECT YOURSELF

The best protection against phishing emails is to remain vigilant. You may receive phishing emails that appear to come from online banks, PayPal, the Inland Revenue or any number of organisations that are connected to your money. A simple defence is never to click on links in emails and then enter any personal or log-in details. Always navigate to the site yourself using your browser.

Avoiding malware is harder because plenty of legitimate websites have been infected in such a way that merely visiting them can run information-stealing code on your PC. If you keep Windows and your applications up to date, though, you reduce the risks massively. Adding anti-malware software is a very good idea, too, but updating your system is arguably the most effective step you can take, and it's free.

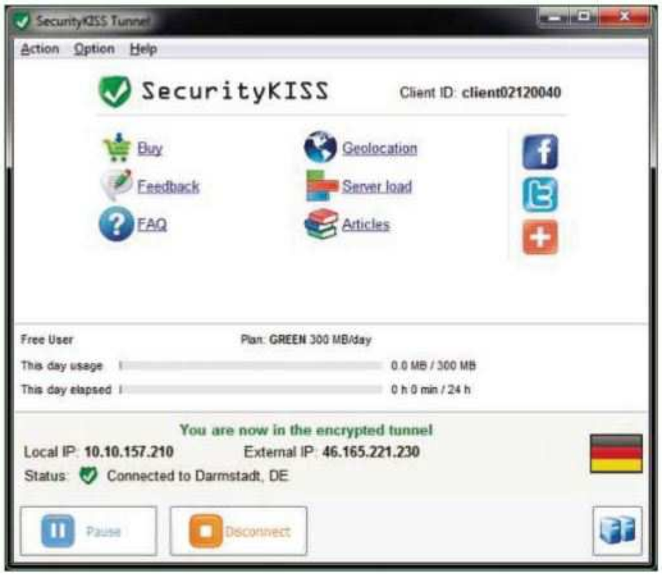
It's not quite so simple to protect your passwords when using wireless networks over which you have no control. Your best bet is not to use public Wi-Fi under any circumstances. If you have a mobile phone that works as a portable hotspot, use that instead. If you need to use public wireless hotspots, however, consider using a virtual private network (VPN) service such as SecurityKISS (www.securitykiss.com), which is free.

LYRICAL LOCKUP

There are many ways to generate strong passwords. A favourite of ours is to take a memorable line from a song or poem and use the initial letters of each word. For example, 'All things bright and beautiful, all creatures great and small' would elicit the password 'atbabacgas'. You can make this more complex by using capital letters and numbers, and by replacing instances of the word 'and' with ampersands. If we capitalise the letters at the end of each line, add a hyphen to separate the lines and use the digit '4' instead of the letter 'a' you'll have: 4tb&B-4cg&S.

According to The Password Meter (www.passwordmeter.com), this is a very strong password with a score of 100 per cent, although admittedly it's not easy to type quickly. Here are some more examples, some of which are better than others. The length, use of capital letters, punctuation and numbers make a big difference to a password's strength.

SONG LYRIC	DERIVED PASSWORD	THE PASSWORD METER SCORE
People are strange when you're a stranger. Faces look ugly when you're alone.	Paswyas.Fluwya.	97 per cent, Very Strong
You're simply the best! Better than all the rest.	Ystb!Btatr.	80 per cent, Very Strong
That ain't workin' that's the way you do it!	Tawttwydi!	61 per cent, Strong
That ain't workin' that's the way you do it	tawttwydi	Nine per cent, Very Weak



Client ID: client02120040

Free User
Plan: GREEN 300 MB/day
This day usage 0.0 MB / 300 MB
This day elapsed 0 h 0 min / 24 h

You are now in the encrypted tunnel
Local IP: 10.10.157.210 External IP: 46.165.221.230
Status: Connected to Darmstadt, DE

Use the free SecurityKISS virtual private network service to stop wireless users spying on your internet traffic, including passwords

This will scramble the passwords and other data you send over the network. There are some security issues when using certain types of VPN over wireless, details of which are available at http://tinyurl.com/vpncons.

If you don't want to go to the lengths of setting up a personal VPN, the very least you should do is ensure that the services you use provide an encrypted connection. Without this, hackers could easily steal your password with a targeted attack. An increasing number of services have seen the light and are providing such connections with options labelled SSL or HTTPS. Both of these mean your web session is encrypted.

Google has provided default SSL encryption for its Gmail service for years, and Microsoft's Hotmail also enables this automatically. Yahoo! Mail, on the other hand, has only offered an SSL option since January 2013 and it isn't active by default. You'll need to enable SSL yourself.

LOCK DOWN YOUR ACCOUNTS

Good security is a matter of striking the best balance between the most stringent procedures and convenience. There's no point in advising someone to maintain 30 different sets of usernames and passwords, with each password over 12 characters long, consisting of alphanumeric characters in both lower and upper case and including punctuation marks. That would be ideal, but it'll never happen.

A more practical approach is to use similar usernames for each account and to have a number of different passwords that you share between accounts, with minor variations. For example, your email username could be Gillian.K234 and your password might be happyshopper1978. Consider using the same username for your Skype account but a variation of the password, such as happyshopper2013.

It's not a bad idea to have the same username for your email and internet messaging services because people will see your username when they write you an email or send you a

TRACKING AN EMAIL

If friends complain they're receiving spam email from you, it means that either your PC or your email account has been hacked – but how do you know which? Email messages contain headers that log the systems through which the message has travelled. These include the identity of the system that sent the message, so you can find out if it's your PC or your email account that has been compromised. You'll need to compare a genuine message sent from your PC with a spam message received by one of your contacts.

You need complete copies of the original messages received by a friend. If your friend forwards them to you, the header information is removed, so instead they need to view the entire message and copy and paste it into another email, or paste it into a text file and send it to you.

To see the full message in Gmail, open it, click on the drop-down menu next to the Reply button and choose 'Show original'. To do the same in Hotmail, open the Inbox, right-click on a message and choose 'View message source' from the list.

The headers we're interested in are labelled 'Received: from'. There will probably be several, but we want those nearest the bottom of the list. In this real example, the legitimate sender was connected to the internet from a Seattle IP address (64.40.54.xxx).

```
Delivered-To: si@h@k.me
Received: from [64.40.54.xxx] by web162904.mail.bf1.yahoo.com
via HTTP; Mon, 14 Jan 2013 10:44:51 PST
```

Let's compare the headers of this legitimate message with those of the spam email that was received by the same friend:

```
Delivered-To: si@h@k.me
Received: from [77.255.73.226] by web162906.mail.bf1.yahoo.com
via HTTP; Mon, 14 Jan 2013 04:15:46 PST
```

By comparing the two, we can clearly see that this message was sent from a different IP address (77.255.73.226), which is based in Warsaw, Poland.

In both cases, the account was accessed using Yahoo! Mail's web interface. We can guess this from the mail server's name (web162906.mail.bf1.yahoo.com), which includes the words 'web', 'mail' and 'yahoo'. The part of the header that says, 'via HTTP' confirms that it's a web interface and also that the connections are not encrypted. If they were, you'd see ''via HTTPS'' instead.

Now that we know these details, we can see that messages from the attacker were sent using the Yahoo! Mail web interface in Poland, while the account owner's PC was in Seattle. There is no reason to suspect that his computer was directly involved in the account's compromise. If the IP address revealed in the spam messages matches your own, it's quite likely that your computer has been co-opted into a botnet. Check your security software immediately, run a full scan of your PC and see if it finds anything untoward. If nothing is discovered, you'll have to seek further help from a local computer shop or repair service.

message over Skype. The username is a personal identifier rather than some obscure piece of information. You should use a different username for your online bank, though, as no one needs to know that information except you and the bank.

It's dangerous to use the same password for every service, though. Not every website stores passwords safely and, as security researcher Troy Hunt discovered recently, Tesco appeared to be storing customers' passwords unencrypted. In this case, if an attacker were to download a list of customer details he would probably be able to see an email address and a password for each Tesco account. If someone were to use the same password for their Tesco and email accounts, the hacker would be able to access and even hijack their email. There is a website that tracks services that don't encrypt users' passwords. You can find it at http://plaintextoffenders.com.

Some people recommend that you change your passwords regularly, and some services require this, forcing users to use unique passwords every few months. For most of us, this only makes sense if we use the same passwords across multiple accounts, which we've established is a bad idea. Instead, spend your energy in building and maintaining a good list of usernames and passwords that work with one account each.

If you have only one email account, we strongly advise you to set up a second. If you maintain two secure email accounts you can use one as a backup for the other. This is handy, as we'll see when we look at recovering a hacked email account.

Check to see if each service you use has an option to encrypt the connection. As we mentioned earlier, Gmail and Hotmail use SSL/HTTPS by default. Other services also secure your communications. Twitter now uses encryption by default, although Facebook doesn't – you have to turn it on in the Security settings by enabling the Secure Browsing option. For Yahoo! Mail the 'Turn on SSL' option can be found

STRONG PASSWORDS

Once you've generated your passwords and associated them with your usernames, write the pairs in a notebook. This may seem controversial, but there's a vast difference between someone hacking your account from Poland, say, and accessing the contents of your kitchen drawers. As long as you keep the notebook away from your PC to foil burglars, there's little that compares for reliability and ease of use.

An F-Secure blog post from 2009 explains a clever idea for generating and remembering passwords that relies on writing down part of the password that's hard to remember. You then add a private 'PIN', which you memorise, to complete the password. For example, your Amazon password would consist of three parts: the first is AMA (for Amazon), the second is random digits and the third is your PIN (for example, b&b). The result would be AMAjyw3fiub&b (which is very strong). Write down AMAjyw3fiu. By looking at your list of passwords, you can tell that it's your Amazon one, but as only you know to append b&b it's useless to anyone else. Full details are available at http://tinyurl.com/passpin.

in the Mail Options menu. Note that there's no technical disadvantage to using SSL, so always use it when you can.

Online backup services such as BackBlaze transfer data from your computer to their servers over encrypted connections. However, in many cases, the data is encrypted in such a way that the company can access the files' contents. You may trust the company, but can you be sure it will never be hacked? History tells us that we shouldn't assume as much.

With BackBlaze, you can choose to add an additional layer of encryption that locks the files' contents away from everyone, although this also means that if you forget the password you've lost the files. Consider writing down the password and keeping it somewhere safe. Hackers might attack your online backup service, but they're unlikely to burgle your house for your password, too.

TO HAVE AND TO HOLD

So far, we've combined common sense with a couple of tips, but we can raise the bar even further by following the advice that Google recommends. As well as providing a backup email account, you should register your mobile phone number with as many important services as you can. These will be those that manage your email, personal files (such as online backup), social media such as Twitter and any blogs you write.

If you use your Google account for email, Google+, Google Docs and other services, you only have to register your phone once. Go to https://www.google.com/settings/security and follow the instructions. For other accounts, you'll need to hunt through the account and security settings pages. We've printed the name and web address of the two-step verification settings for common services in the box on page 108.

Once you've registered your phone with a service, you potentially have access to a second level of authentication. When you log in using your username and password, the website may require you to enter a further code, which it sends as a text message to your phone. This is one of the most practical ways of using two-factor authentication, also called two-step verification.

Two-factor authentication has had a patchy record. It's a great idea in theory but it can be very inconvenient. Some high street banks already require customers to use a special dongle to log into their online banking systems, but if you don't carry the device around with you and you find that you want to log on when you're away from your desk, you're out of luck. Even in business these devices can cause problems. We once met a furious security expert abroad who was fuming because he was locked out of his email. The IT department had issued new smartcards for authentication but, as he'd been travelling for so long, he'd been unable to collect his.

Using a mobile phone is a good compromise, and it's far more realistic to expect consumers to carry a phone with them than half a dozen different USB keys, smart cards and other chipped devices. If you have a smartphone, you don't even have to rely on a mobile network connection. Software such as Google's free Authenticator application provides codes for a range of services. Google Authenticator works on Android, iOS and BlackBerry devices and provides secure authentication for Google's services, Dropbox, at least one web hosting company and content-management systems including Drupal and WordPress.

Hotmail doesn't support this type of software-based authentication, but it does allow you to log in using a code sent to your phone. Don't be fooled into thinking that this amounts to two-factor authentication, though. If you don't also need to use your password, it's just an alternative way of accessing your account. Its main purpose is to help you if you forget your password. You certainly should guard your phone carefully if you enable this option. ■

CHAPTER 8

8

THE CLOUD

Now that we've gone pretty much exclusively digital, backups have never been so important. Without the right backup procedure in place, you could easily lose your precious digital photos, videos, music and documents forever. Fortunately, the cloud is here to help. By storing everything online you remove the threat of fire, theft and mechanical failure, giving you an incredibly simple way of protecting your files. Here we look at backups, how to choose the right cloud storage service and how to protect all your files online.

CONTENTS

Keeping your data safe

Cloud storage means that your data is safe from fire, theft and mechanical failure. In this chapter we'll show you how to work out where to back up, how to choose a cloud service and how to use it.

Cloud storage has completely changed how we think about and approach backups. With files automatically stored online the second they're saved, online backups are fast, convenient and immune to the problems of local backups, such as fire, theft and mechanical failure.

That's not to say that cloud backup is perfect and that local backups aren't any use. Local backups are much quicker to make, give you complete control over what's going on, and are a lot cheaper with more storage space. In truth, then, a combination of local and cloud storage is the ideal way to go.

However, before we show you how to use online backup services, we'll look at more general issues surrounding backup. We'll even tell you how to deal with old file formats and media.

Specifically, we'll tell you how long each type of media will last before data becomes unreadable and how to ensure that your backups are kept up to date on current media. We'll also tell you how to deal with file formats, so you don't end up with old documents that you can no longer read. And don't worry if you have old file formats that you currently can't read – we'll tell you how to deal with them.

LIFE CYCLE

With the majority of our important data, including photos and music, now digital, it's more vital than ever to keep backups. While simply copying data from one hard disk to another is a form of backup, it doesn't protect against the theft of your computer or a fire in your home. Backing up to DVD and giving these to a friend is a way around the theft and fire problem, but how long do DVDs last before breaking down?

Making a backup is about more than simply copying the data to other places; you also need to consider how long the backup media will last. Everything degrades over time, and it's possible that your carefully made backups will become unreadable. On these pages, we'll be looking at how you should choose your backup media and how to make sure that it keeps working. Our table *(see page 119)* gives you an overview of what each type of backup media is good for, but we'll cover each format in more detail here. How long each media type lasts for is only an estimate and, depending on the quality of your chosen media, your backups may last for more

Optical discs are a good way to make backups that you'll store outside of your home or for data you don't want to change

A hard disk is a fast way to back up your data and excellent value, but you should upgrade it every five years to keep it up to date

or less time. Regardless of the backup types you choose, it's worth keeping pretty much every file you own on a local hard disk or NAS, so that you have fast access to them when you need them.

OPTICAL MEDIA

CDs, DVDs and Blu-ray discs all have the advantage of letting you quickly create multiple copies of the discs, which can be given to friends or family to store in their homes. This means that if your house were to be robbed or suffer from a fire, you know that you have safe copies stored elsewhere. Out of the three disc types, we have a slight preference for DVDs, as the cost per gigabyte is lower.

Although rewritable discs are available, they're comparatively expensive, so we generally prefer the write-once discs. The only exception is Blu-ray, where the minimum capacity of 25GB can be hard to fill in one go, so rewritable discs may make more sense. The one thing you can't get around is the fact that optical discs are comparatively slow compared to hard disks or NAS devices.

With this in mind, optical discs are best used for backing up data that you don't need to change, such as digital photos and videos you've edited. It's worth creating archives of these important files, perhaps by year (depending on the amount of storage this requires). Make multiple copies of the discs and give some to friends, and keep a set for yourself.

The lifespan of an optical disc depends on the format, but is at least 10 years. At some point, then, it's worth making a fresh copy of the discs. Alternatively, you should copy the files off the discs and use a newer type of media that has better support. Generally speaking, you should check the discs at least once every five years to make sure they're still working.

Solid-state drives are tough and reliable, but their relatively small capacities mean they're not so useful for backups

HARD DISK

Hard disks are brilliant for backups, as they're incredibly fast and come in high capacities. An internal hard disk can be used to store additional copies of files, while an external hard disk makes for a natural and easy backup destination. Because of the high speed of these disks, it makes sense to use them for all backups, including files that may change on a regular basis, such as the contents of your Documents folder. The downside of this type of storage media is that they're likely to be kept at home, so they're more vulnerable to theft or accidents.

If left turned off for long periods of time, a hard disk can lose its charge, although error correction can fix some data degradation. However, the general consensus is that data integrity should be longer than the mechanical life of the hard disk, which is around five years on average.

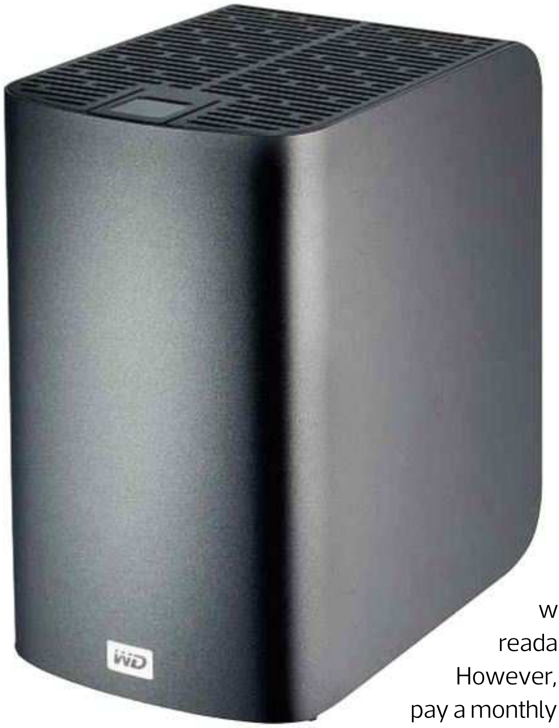
Given the stupendous increase in capacities, five years is long enough for any old hard disk to seem small and out of date. Every five years or so, as you upgrade your computer, it's worth copying the contents of your existing backup hard disk to a completely new one.

SOLID-STATE DRIVE

A solid-state drive (SSD) uses memory chips rather than moving parts, making it faster and more reliable than a mechanical hard disk. The only one potential problem is that the memory cells have a write limit; once this is reached, no more data can be written to that part of the disk, although it can still be read.

With average use, an SSD will last for up to 25 years in a PC, but the data should still be readable for up to 50 years. This makes an SSD sound an excellent choice for backup, but they're expensive per gigabyte. Even with recent price drops, a 500GB SSD still costs around £250. As such, they make good boot drives or laptop hard disks, but for backups they're not good value.

If you do have files stored on an SSD, it makes sense to upgrade the disk when you need more



A NAS device has the same benefits and downsides as a hard disk, but you can easily share the disk space between multiple computers

capacity, as the length of time the data will survive will far exceed the drive's lifetime.

NAS

A NAS is effectively a networked hard disk, so suffers from the same problems as a normal hard disk. It has the benefit that all the users on your network can use it. Storing some files centrally makes a lot of sense, too: with your digital photos, videos and music on a NAS you can quickly stream them over the network. We recommend keeping a copy of your files locally, and a copy on your NAS.

If your NAS supports it, a RAID array can provide an extra level of protection at the expense of total capacity. RAID 1 is the obvious choice, which is mirroring. This requires an even number of hard disks, as data written to one disk is written to another automatically. Should one disk fail, the other is still readable. Replace the broken disk and the RAID array is rebuilt, and you're ready to continue.

As with hard disks, you should look to upgrade or change the disks within five years to ensure you don't lose any data.

ONLINE BACKUP

Off-site data storage should be an essential part of any secure backup routine and the easiest approach is to use an online backup service. Managing a local backup routine can be a chore that often gets postponed and forgotten about, but online backup, which keeps all your files in the cloud, is usually a set-and-forget affair.

It's also more secure than local backup. Because the data is taken off-site, you'll still be able to recover it in the event of fire, flood or theft. Now that broadband is so fast and cheap, it's realistic to back up all your data online. You can also use synchronisation services to make sure that the work you want to take home gets there long before you do, enabling you to access your data wherever you are.

The company that runs the service will ensure that your data is always readable, making it less hassle for you. However, the downside is that you have to pay a monthly or yearly fee. If you fail to keep up payments, you lose access to your files.

The other potential problem with online backup services is that if the provider goes bankrupt, there's a good chance that you won't be able to access your data, unless the company is bailed out or bought by another firm. For this reason, online backup is worth using in conjunction with at least one other method here, although it should be your primary method as it's secure, quick and convenient.

> “Managing a local backup routine can be a chore that often gets forgotten about, but online backup is usually a set-and-forget affair.”

CHOOSING AN ONLINE BACKUP SERVICE

The most obvious factor when choosing your backup service provider is how much storage you get for your money. This can vary widely, with some providers offering just 20GB of space, while other services provide hundreds of gigabytes or even unlimited storage for around the same price. However, some companies that offer unlimited storage impose other limits on the data you upload, by not supporting external drives or certain file types, for example.

Services with fixed-capacity allowances tend to be more relaxed about how you use them, with support for multiple computers on a single account. Most users have only a couple of gigabytes of important personal files, but you'll need more space if you want to back up lots of photos, videos or audio files. Often the limiting factor isn't how much space you have available to you online, but the length of time it would take to upload, say, 100GB of data.

Most home broadband connections have an upload speed of between 450Kbit/s and 1.5Mbit/s. It might take around 14 minutes to upload 30MB of data over a basic home ADSL connection, while a Virgin cable connection with an upload speed of 1Mbit/s can manage the same task in around seven

FORMAT WARS: KEEPING BACKUPS UP TO DATE

Formats rapidly go out of date, and you may find if you buy a new computer that it no longer supports your chosen backup media. Remember how quickly floppy disks went out of fashion? When you upgrade your computer, always check that the new one supports your old backup media. If it doesn't, you'll need to upgrade your backup media using your old PC while you still can.

Then there's the issue of physical file formats. As developers improve the quality of their software, so they introduce new file formats. Over time, the old file formats become unreadable. For this reason, if you upgrade your software, check that it will read your old file formats. If it won't, use the previous version that worked to open your files and save them in a newer, better-supported format instead.

For digital photos and music, we recommend using well-supported standards that are likely to stay in date for a long time, such as MP3 or WAV for music and JPEG or PNG for photos. That's not to say that you shouldn't keep your RAW camera files, for example, but just make sure you've also got a copy in a better supported format.

If you have data backed up on ageing media, such as Zip discs, or in little used formats, make the time to copy your files to new, more future-proof storage. Just transferring the data to a hard disk directory linked to your online backup service is a good start, but you should copy really important files to DVDs, which you can then send to a friend or relative for safekeeping.

If you have old backup disks in a format that you can no longer read, such as 5¼in floppy disks, you may have to consult a recovery specialist to get your files back. Be aware that if your disks are also damaged, the recovery costs could be astronomical, so it may not be worth the effort.

Ageing file formats are more of a problem. If you can still run the software that created the files, make sure you export a copies in a more universal format. RTF is a good bet for text documents, for example, while PDFs are best for rich files from DTP programs.

If the software that created the files isn't compatible with current versions of Windows, you might be able to run it using a virtual machine. Virtual machine images of everything from Windows 3.1 onwards are available for programs such as VMware Player (www.vmware.com/products/player) and VirtualBox (www.virtualbox.org), while DOSBox (www.dosbox.com) provides an environment for running even older software.

Even when it comes to current programs, be aware that proprietary formats can last only as long as the software that created them. If you're recording all your music masterpieces as proprietary project files in Digital Audio Workstation format, for example, it's a good idea to export individual tracks in WAV format to ensure that you'll still be able to edit them even if the maker of your software goes out of business.

minutes. At these speeds, 100GB would take 16 to 32 days of continuous uploads, and much longer if you wanted to switch your PC off at night or if the broadband supplier throttled the connection due to excessive use. If you have a fibre connection, though, you could see upload speeds of around 15Mbit/s or more, reducing that 100GB upload time to just 16 hours. Bear in mind that if your ISP caps your monthly bandwidth, your backup and synchronisation tasks could have a major impact on your limit.

If you have a lot of data to back up or restore at once, it may be worth choosing a company that lets you post a DVD or hard disk rather than shifting gigabytes of data over the internet. This could prove critical if you need to restore more data than your broadband connection will allow, or you simply wish to carry out a full restore without any delay.

SYNCHRONISATION SERVICES

As well as online backup services, you could also consider synchronisation services, which help you keep multiple devices up to date with the same files, while storing a secure copy online in your cloud storage.

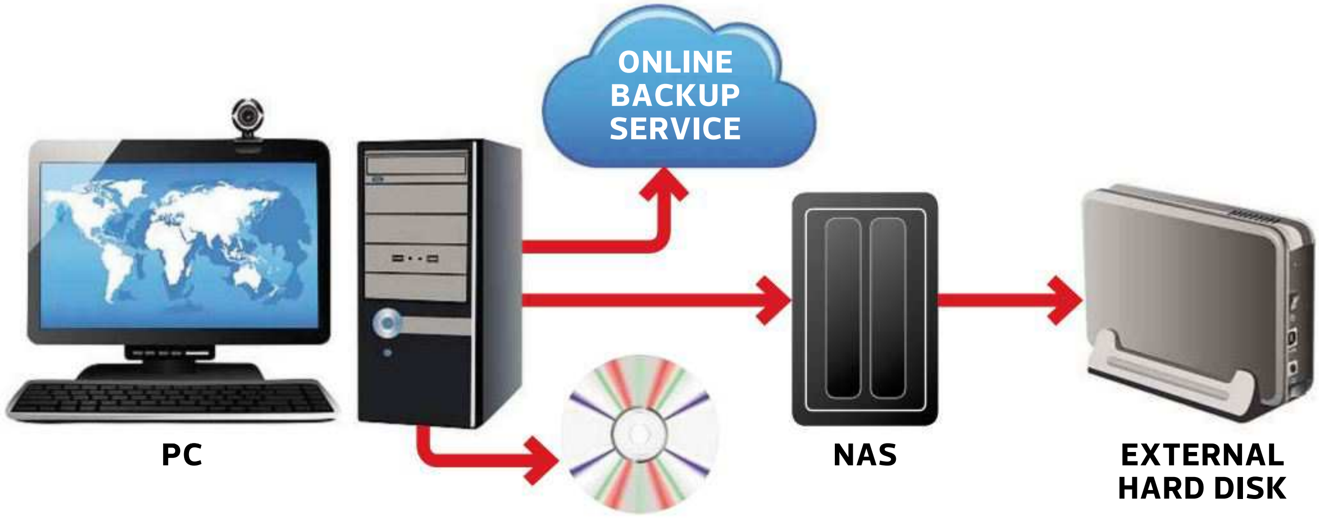
Once your files are stored securely online, you get a secondary benefit: the ability to share files. This can often be done through the desktop client, but you'll usually find the same options via the web client, which lets you access your files from any computer with a web browser.

The most limited synchronisation services only allow you to email links to individual files; others provide a full multimedia browser that not only lets you share entire directories but also incorporates photo galleries or a streaming facility for your audio and video files. Many services also allow you to access and even upload files directly from your mobile phone or tablet.

Most synchronisation and backup services will retain old or deleted version of files. Version retention can be a lifesaver if you've accidentally deleted or mangled a section in an important document, whether it's your financial records or the first draft of your novel. Some services keep only a few versions, such as the last five saved copies. However, as most

➔

DATA SECURITY: SETTING UP YOUR STORAGE



A comprehensive and secure backup system needn't be complex to set up. Start with an online backup service and specify the directories you wish to back up. Make sure you know exactly how much data you'll be backing up online and ensure that both your account and internet connection are up to the task.

In addition to a remote backup to online storage, you should also make local backups. The simplest option is to connect a NAS or external hard disk and use a backup application. We recommend using Acronis True Image (£30 inc VAT) or Paragon Backup & Recovery Free to schedule regular backups. A few online backup services, such as SOS Online Backup and MozyHome, also have clients that can back up to local, external or network drives. Other free backup tools include DataBarracks BuddyBackup, which allows you and your friends to store encrypted online backups on each other's PCs. However, because your friends can opt to remove your backup privileges at will, this is far less secure than going for a commercial backup service.

Some recent NAS devices can also back up their contents to the cloud thanks to packages available for download from their maker or from third party sites. Large-scale business services such as Amazon's S3 servers are widely supported, but support for consumer services is limited. Western Digital NAS devices have recently introduced support for Dropbox, though, while iDrive has released an app to allow you to back up QNAP NAS devices to its online storage.

Finally, you can back up the NAS – or selected directories on it – to an external hard disk. Almost all NAS devices have their own scheduled backup tool to regularly copy some or all of their data to a drive connected over USB. If you're making business backups, then the additional disk is useful if you have sensitive data that you wish to be able to take off site. A weekly or daily rotation of two external disks is best for this, with one disk being outside the building at all times. For more personal content, assuming your external drive is formatted using a reasonably common file system such as FAT32, the external disk means that you can always have your favourite pictures and music backed up on an easily portable medium.

Photos and music can also be copied to DVDs, perhaps on an annual basis. Multiple copies make sense, so you can store a copy of your files at a friend's or relative's house, protecting your data against damage in your own home.

of us are in the habit of saving frequently, this might not be enough before you notice your mistake. A few services, including SquirrelSave, Dropbox and SOS Online Backup, can provide version storage over an unlimited period, which is worth having if you need extra peace of mind. Before you choose a service, you should find out how long the company retains deleted copies and how it handles version retention.

Online backup and synchronisation is a highly competitive market, with dozens of large and small companies. Because of this, and because of the need to impress prospective customers, many providers offer free as well as paid-for services. A number of companies also offer time-limited trials so you can try out the service before committing to it, so it's worth doing a bit of online research first .

DO IT FOR FREE WITH GOOGLE DRIVE

There are a number of online backup and synchronisation services available, but it's worth noting that the majority of internet users are already signed up to one. If you have any kind of Google account, whether you use it for your Android phone, email or blogging, then you already have a massive 15GB of online storage available to you.

For many people, it's as much remote storage as they're ever likely to need. There's even versioning: old versions of files are automatically deleted after 30 days or 100 revisions, but you can opt specific files out of this, which is useful for critical documents. Many file types can be previewed and even converted for editing in Google Docs.

There are a couple of disadvantages to using Google Drive. First, only your local Google Drive folder is synced: you can't add other directories. The Google Drive web interface's default My Drive view lumps all the files you own into a single list. This can also be overwhelming, but you can view files by folder if you select Folders under 'Owner, type, more' in the left-hand panel. Finally, the way Google has divided its service means that there's no integration between content you upload to Google Drive and other services, such as the slick audio streaming of Google Play Music or G+ photo albums. While this would be welcome, it doesn't detract from Drive's core functionality.

It's not perfect, but Google Drive's ubiquity means it's often the easiest way to share everything from business documents to directories full of photos. Just copy the files or folders you want to share to your Google Drive desktop folder or drag them to the Drive web interface. Once they're uploaded, select Share from the Google Drive website's right-click menu and choose who you want to have access to your content.

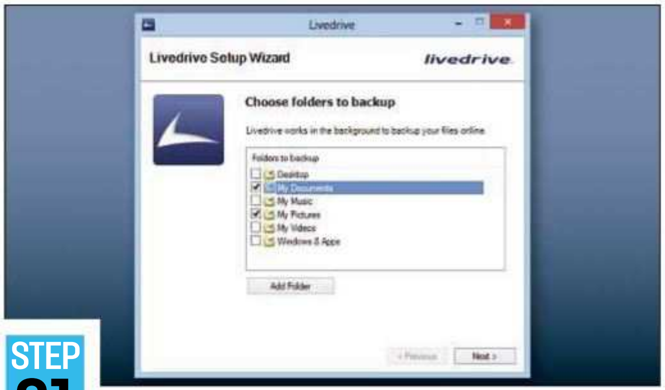
HOW LONG YOUR BACKUP MEDIA WILL LAST?

MEDIA	LIFESPAN	PROS	CONS	GOOD FOR
CD	10 years	Cheap; multiple copies can be easily stored in different locations	Low capacity	Digital photos
DVD	20 years	Multiple copies can be easily stored in different locations	Relatively low capacity	Digital photos and videos
Blu-ray	100 years	High capacity; multiple copies can be easily stored in different locations	Expensive	Digital photos and videos
External hard disk	Five years	Relatively cheap; fast; easy to duplicate; can take off site	Likely to stay at home, so vulnerable to fire and theft	Digital photos, music, videos and files
Internal hard disk	Five years	Relatively cheap; fast; easy to duplicate	Vulnerable to fire and theft; can only be stored locally	Digital photos, music, videos and files
Solid-state drive	50 years	Fast; once write limit has been reached the data is still readable	Expensive; vulnerable to local fire and theft	Digital photos, music, videos and files
NAS	Five years (with hard disks installed)	High capacity; often has RAID protection; easy to share with family	Vulnerable to local fire and theft	Digital photos, music, videos and files
Online storage	Forever	Constantly kept up to date; immune to physical theft, fire and other accidents at your property	Cost of paid services adds up; if the company goes bust you lose your data	Digital photos, music, videos and files

How to use cloud backup

With a cloud backup service, you can save all your important files online. Properly configured, cloud backup will make sure that you never lose another file ever again.

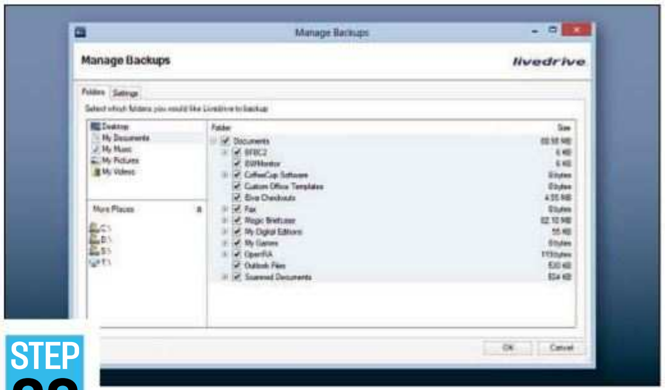
In this walkthrough we'll show you how to get everything up and running quickly and easily. For the purposes of this



☐ Desktop
☑ My Documents
☐ My Music
☑ My Pictures
☐ My Videos
☐ Windows 8 Apps

STEP 01 SET UP INITIAL BACKUP

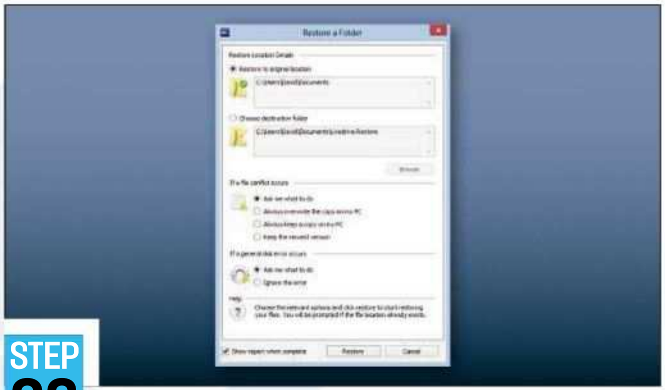
The initial setup wizard lets you choose the folders that you want to back up. Livedrive gives you a list of default folders, such as My Music and My Documents, but click on Add Folder and you can choose a specific location. Put ticks next to all the folders you want to back up, and then click Next. The software will finish configuring itself and start backing up your data automatically.



☑ Documents
☑ BFBC2
☑ BWMonitor
☑ CoffeeCup Software
☑ Custom Office Templates
☑ Elva Checkouts
☑ Fax
☑ Magic Briefcase
☑ My Digital Editions
☑ My Games
☑ OpenFIA
☑ Outlook Files
☑ Scanned Documents

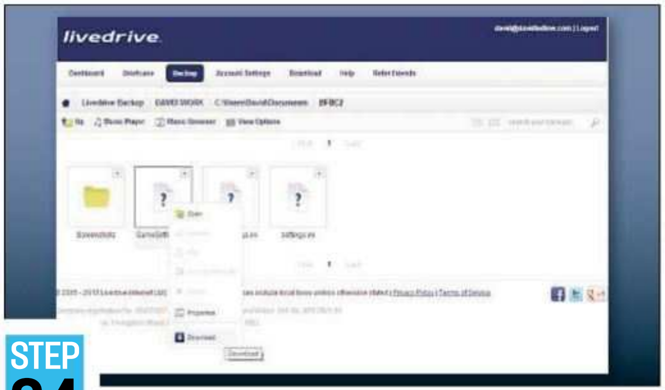
STEP 02 MANAGE FOLDERS

Folders can easily be added to your backup. In Windows, right-click on a folder in Explorer and select the backup option from the Livedrive menu. You can also right-click on the Livedrive icon in the Notification area and click Settings, Services, Manage Backup. Any folder with a tick next to it is being backed up, so remove the tick to stop it being backed up (this will also delete any backed-up files). Put a tick next to any blank folder to add it to your backup.



STEP 03 RESTORE FILES

In the Settings menu, click Services and Backup Restore. This opens a similar window to the Manage Backup folder. Here you can select a file or folder and click Restore. Livedrive will ask you where you want to restore the file to. The default location is the original folder, but you can click Choose destination folder to restore the file to a different location. Click the Restore button when you're done.

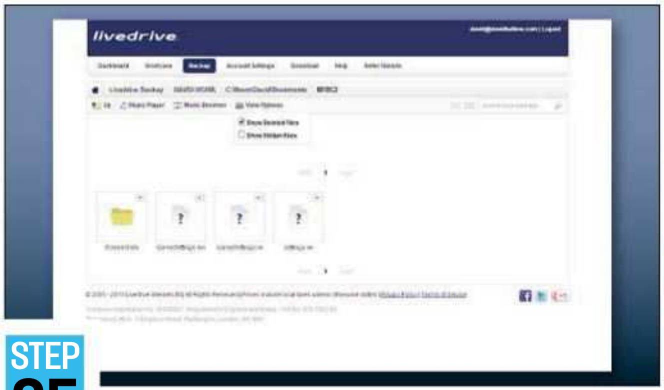


STEP 04 ONLINE ACCESS

You can access your files from any internet-connected computer at www.livedrive.com. Although you can't download folders from here, you can download individual files. To do so, just right-click on the file you want to save, click Download and it will be saved to your computer.

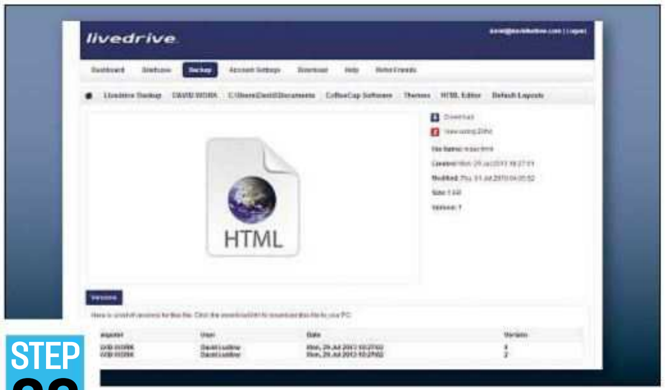
tutorial we're using Livedrive (www.livedrive.com), which offers unlimited storage space for a single PC. It works quietly in the background to protect your files as you use your computer. Other backup services have similar features, but check the instructions for your service carefully if you're using a different cloud-based provider.

You'll need to register for an online backup service online. This will involve creating a username and password. You'll need to remember these, as this combination will be required if you need to restore your computer at a later date. Once you've set up your account, download the client for your computer and install it. There are clients for both Windows and Mac OS X.



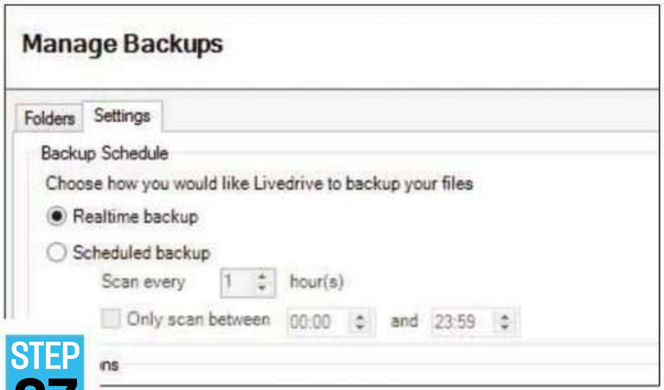
STEP 05 DELETED FILES

If you delete a file, it's removed from your online backup. If you do this by mistake and need to get a copy back, don't panic. Livedrive saves deleted files for 30 days. To restore a file, just go to the web console and browse to your computer. Click View Options and select Show Deleted Files. Then navigate to the folder where the file was and you'll be able to download it.



STEP 06 VERSIONS

Livedrive also keeps multiple versions of your files, so don't panic if you accidentally overwrite an important document, as you can get it back. Just go to the web interface and browse to the file you need to restore. Double-click the file to display a properties screen. At the bottom you'll see a list of versions, organised by date and time. Click the one you want and click Download to save it to your computer.



Manage Backups

Folders | Settings

Backup Schedule

Choose how you would like Livedrive to backup your files

● Realtime backup

○ Scheduled backup

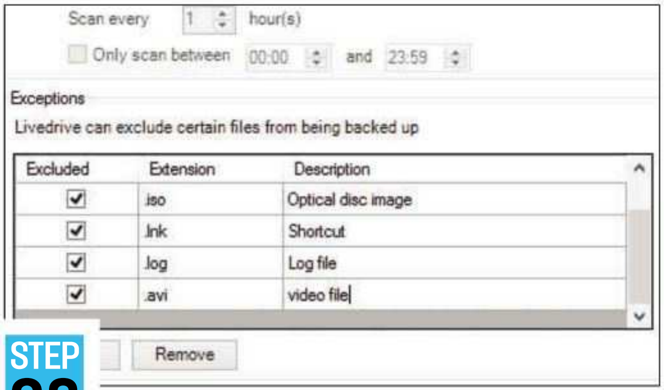
Scan every 1 hour(s)

□ Only scan between 00:00 and 23:59

ns

STEP 07 TAKE CONTROL

By default, Livedrive backs up your files once every hour. However, you can change this if you're doing a lot of work and want to make sure your files are backed up more regularly. Go to the Settings app on your computer and click Services, Manage Backup and then click the Settings tab. If you chose Realtime backup, Livedrive will save a file every time it's changed. If you prefer to leave it to a schedule, you can use the options to pick when your files will be backed up.



Scan every 1 hour(s)

□ Only scan between 00:00 and 23:59

Exceptions

Livedrive can exclude certain files from being backed up

Excluded	Extension	Description
☑	.iso	Optical disc image
☑	.lnk	Shortcut
☑	.log	Log file
☑	.avi	video file

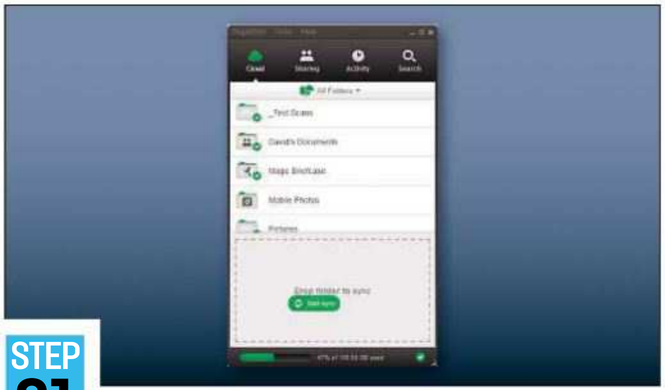
STEP 08 EXCLUDE FILES

On the same Backup Settings page you can also choose which files to ignore. By default Livedrive ignores files with .exe, .iso, .lnk and .log extensions. You can remove the tick from their boxes to back them up, and you can also add your own exclusions. For example, you may not want to back up video files. Click Add to add your own custom file type, then add the extension of the file to exclude followed by a meaningful description. Click OK when you're done.

How to synchronise your files

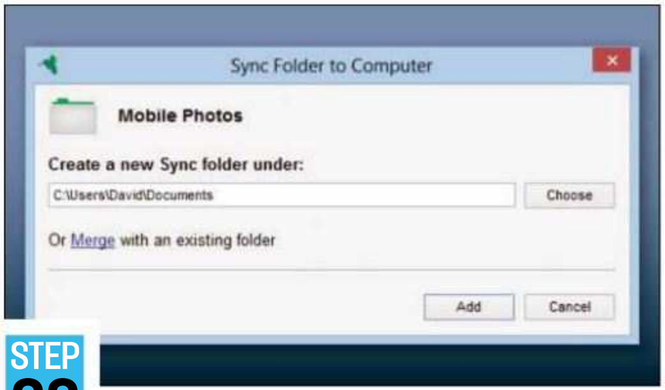
If you need to keep files up-to-date on multiple computers, synchronisation software is the way to go. We'll show you how to do it using the cloud.

Cloud synchronisation tools are a brilliant tool for keeping files up to date on multiple computers. They work by saving a file to the cloud every time it's changed; each



STEP 01 ADD A FOLDER

Skip the setup wizard and launch the control application by right-clicking the Notification icon and clicking Open SugarSync. To select a folder to synchronise, drag and drop the folder into the SugarSync window in Windows Explorer. This will automatically start backing up all the files in that folder. Any changes to those files are then automatically saved online. The Magic Briefcase folder is shared automatically and is handy for notes and other important information.


Sync Folder to Computer

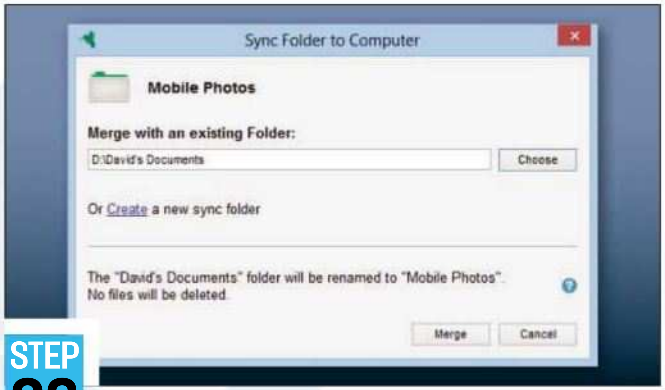
Mobile Photos

Create a new Sync folder under: C:\Users\David\Documents

Or Merge with an existing folder

STEP 02 SYNC TO ANOTHER COMPUTER

To synchronise your folder to another computer, install SugarSync on it and open the control application as in Step 1. Under Cloud, you'll see a list of folders . Click the folder you added in Step 1 and select the toggle button next to 'Now syncing to this computer'. In the next window, you'll see 'Create a new Sync folder under' followed by a location on your hard disk. A new folder with the same name as the synced folder is created at that location. You can change the location by clicking Choose.


Sync Folder to Computer

Mobile Photos

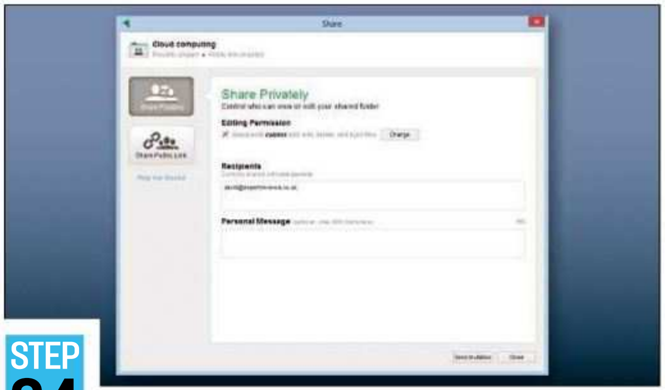
Merge with an existing Folder: D:\David's Documents

Or Create a new sync folder

The "David's Documents" folder will be renamed to "Mobile Photos". No files will be deleted.

STEP 03 MERGE FOLDERS

You don't have to create a new folder for synchronised cloud folders. Instead, when you turn on synchronisation you can click Merge instead. This lets you save the synchronised folder to a folder of your choice, merging the contents of both. For example, you might have a folder called Photos on one computer and Pictures on another; Merge lets you join the contents of both. Repeat Steps 1 to 3 as many times as you need for your folders and computers.


Share

Cloud computing

Share Privately

Editing Permission

Recipients

Personal Message

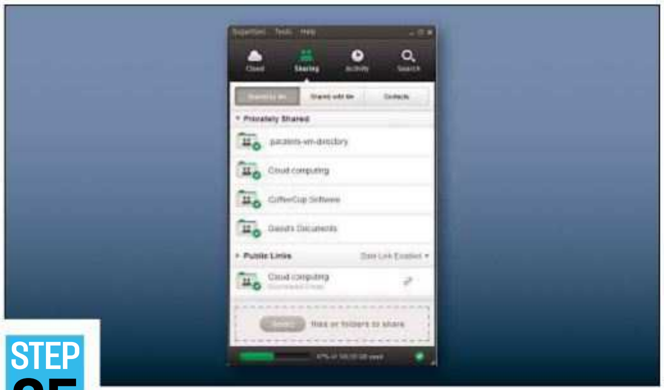
STEP 04 SHARE FOLDERS

SugarSync also lets you share files and folders. Folders can be shared publicly, where a public web link can be used by anyone that has it, or privately, letting people you choose edit the files. Right-click on the file or folder you want to share and select Share from the SugarSync menu. Public links only let people download files, not edit them. For private links, you can choose if people can edit the files as well as view them, but the recipient must have a SugarSync account to access the folder.

computer the file is synchronised to then downloads the latest version next time it's turned on. That means you can start work on a presentation on your work computer, shut it down and turn on your laptop at home, continuing to work where you left off.

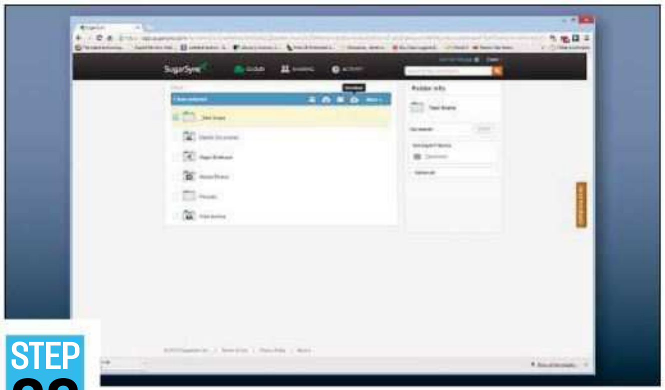
We'll show you how to use SugarSync, which is an advanced synchronisation tool, although similar principles are used for other services. There's a free 5GB version, which you can get by signing up at www.sugarsync.com, but you can also buy more storage if you need it.

Once you have a SugarSync account, you'll need to download the client software, which is available for both Windows and Mac OS X.



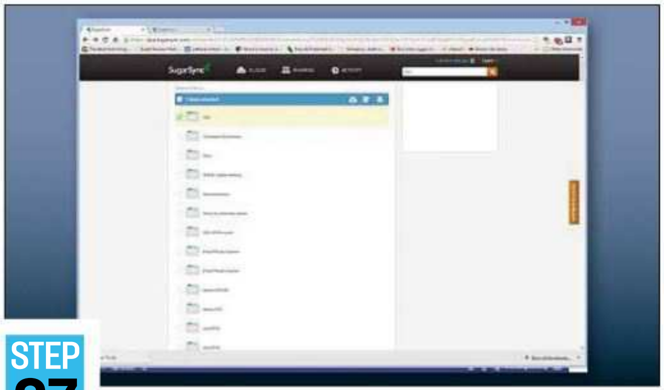
STEP 05 MANAGE SHARES

From the SugarSync app you can click on Sharing to view all Shared folders. The default view is Shared by me, which is the folders you're sharing; you can also view Shared with me. Under Shared by me you can manage all your public links. Right-click on one to copy the link or to remove it. For private links you need to click on the folder, then you can remove permissions for people or invite new people to share it.



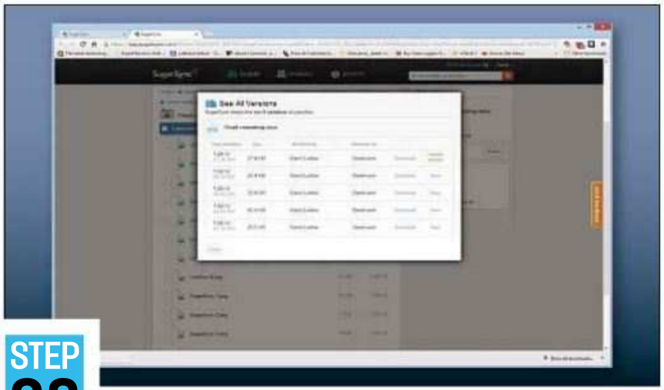
STEP 06 ONLINE ACCESS

You can view your files through the online account, too. Just go to www.sugarsync.com and sign in. Here you can browse through all your synchronised folders . Put a tick next to a folder or file and you can choose to share it or download it. Folders are automatically zipped and downloaded to your computer, so it's a great way to access files if you're on a computer that doesn't have the SugarSync client.



STEP 07 DELETED FILES

SugarSync automatically saves deleted files. They count towards your total storage limit, so you should clear them out every now and then. However, they're useful to have as you can recover a file that you've accidentally wiped. From the web account click on your username and select deleted files. You can sort this list by name or date deleted. Put a tick in the box of the file or folder you want to restore, then choose to download the file, restore it to its original location or delete it.



STEP 08 VERSIONS

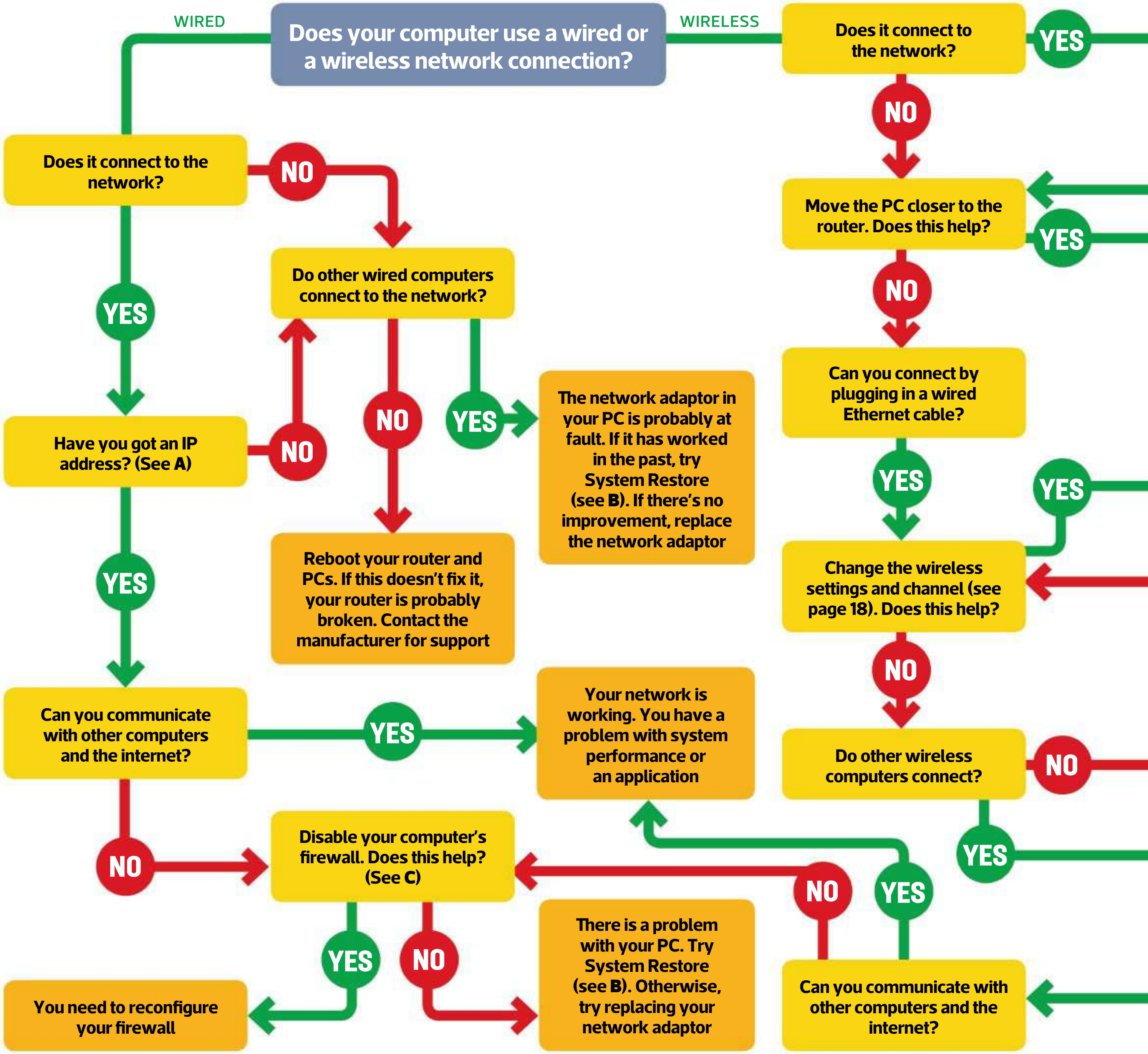
SugarSync automatically keeps up to five versions of each file, so you can restore a previous version if you realise you've overwritten something important. The easiest way to get at the versions is to browse to the file using Windows Explorer, then right-click and select View versions from the SugarSync menu. This loads the web version and shows you all of the versions available. You can simple download the version you want to restore.

9

TROUBLESHOOTING

Having trouble with your home network? Don't worry: our troubleshooting guide will get you to the root of the problem in an instant, so you can get things up and running smoothly again with the minimum of fuss. And if you don't understand some of the technical terms we've used throughout this book, we're also here to help with our jargon-busting glossary.

Fixing your network



Does your computer use a wired or a wireless network connection?

Does it connect to the network?

Do other wired computers connect to the network?

Have you got an IP address? (See A)

The network adaptor in your PC is probably at fault. If it has worked in the past, try System Restore (see B). If there's no improvement, replace the network adaptor

Reboot your router and PCs. If this doesn't fix it, your router is probably broken. Contact the manufacturer for support

Can you communicate with other computers and the internet?

Your network is working. You have a problem with system performance or an application

Disable your computer's firewall. Does this help? (See C)

You need to reconfigure your firewall

There is a problem with your PC. Try System Restore (see B). Otherwise, try replacing your network adaptor

Does it connect to the network?

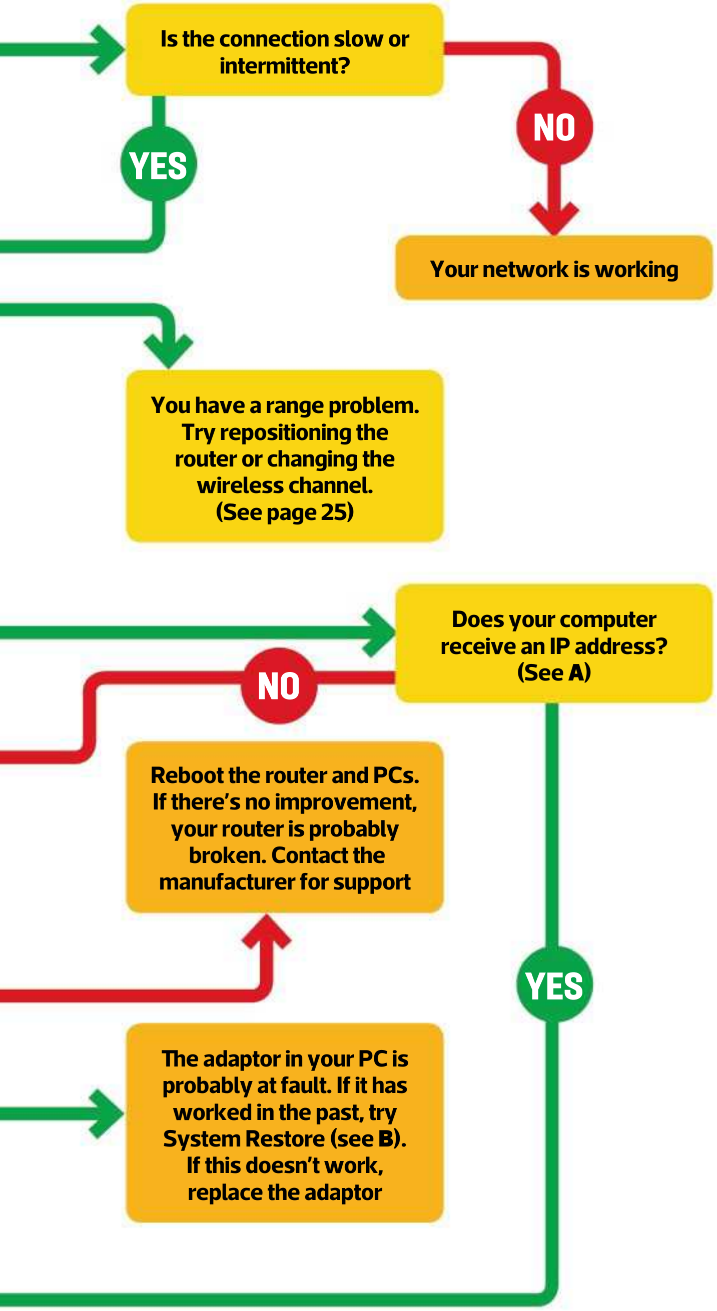
Move the PC closer to the router. Does this help?

Can you connect by plugging in a wired Ethernet cable?

Change the wireless settings and channel (see page 18). Does this help?

Do other wireless computers connect?

Can you communicate with other computers and the internet?


Is the connection slow or intermittent?

YES

NO

Your network is working

You have a range problem. Try repositioning the router or changing the wireless channel. (See page 25)

Does your computer receive an IP address? (See A)

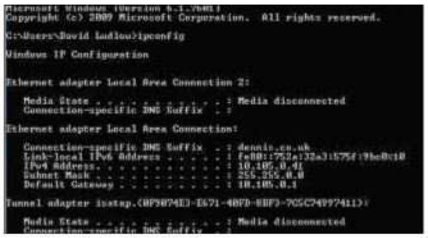
NO

Reboot the router and PCs. If there's no improvement, your router is probably broken. Contact the manufacturer for support

YES

The adaptor in your PC is probably at fault. If it has worked in the past, try System Restore (see **B**). If this doesn't work, replace the adaptor

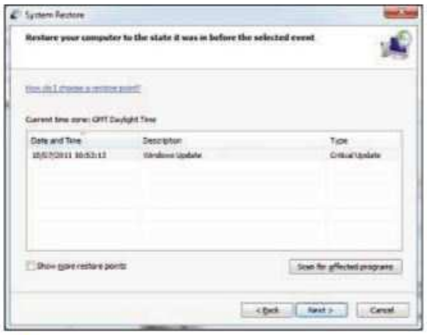
A Your computer or device must have an IP address in order to work. Checking to see if you have a valid address is easy in Windows (you'll need to check the manual for other products). Open a Command Prompt from the Start menu and type ipconfig. If the IPv4 Address starts 169.x.x.x, your computer hasn't received an IP address. You can try restarting your computer and the router to make it obtain a new address. Alternatively, you can type ipconfig /release all followed by ipconfig /renew to force your computer to get a new address.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\David Ludlow>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : dennis.co.uk
   Link-local IPv6 Address . . . . . : fe80::752a:32a3:575f:9be0%10
   IPv4 Address. . . . . . . . . . . : 10.105.0.41
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.105.0.1

Tunnel adapter isatap.{0F9074ED-E671-40FD-88F3-7C5C74997411}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Find out if your computer has an IP address using a Command Prompt

B System Restore takes your computer back to an earlier working state. You can run System Restore from the Start menu. In Windows 7 and 8, click Next, then click 'Show more restore points'. Select the restore point from when your PC was working properly, and click Next. For older versions of Windows, select 'Restore my computer to an earlier time', click Next and use the calendar view to select an appropriate restore point. Click Next to apply the changes.



Restore your computer to the state it was in before the selected event

How do I choose a restore point?

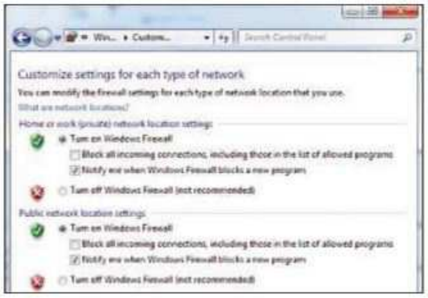
Current time zone: GMT Daylight Time

Date and Time	Description	Type
15/07/2011 10:52:12	Windows Update	Critical Update

□ Show more restore points

Use System Restore to fix problems

C An incorrectly configured firewall can stop your computer connecting to the internet. To turn off the Windows firewall in Windows 7, run Windows Firewall from the Start menu. Select Turn Windows Firewall On or Off, then select Turn off Windows Firewall for both Home or work and Public networks. Click OK. For older versions of Windows, go to the Security Center and click the Windows Firewall link at the bottom. Click Off and then click OK. If you're using a third-party firewall, such as the one that comes with your security suite, you'll need to read its instructions to find out how to disable it.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

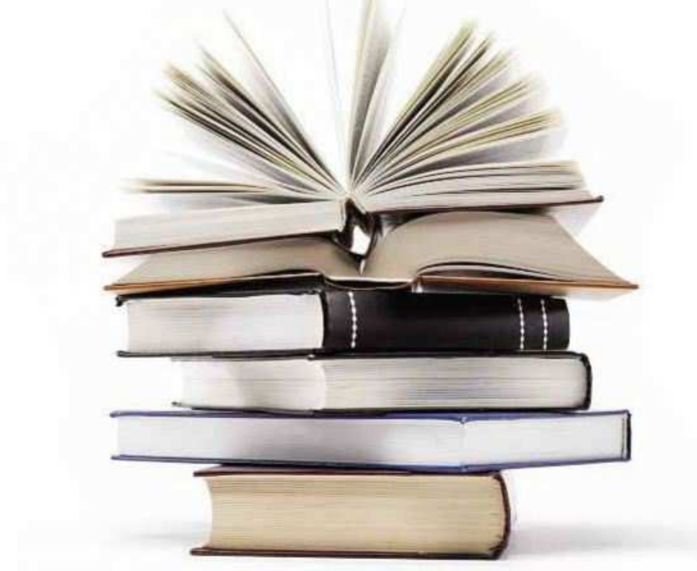
● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Try turning your firewall off if your PC can't connect to the internet



Glossary

2.4GHz The standard radio frequency band that wireless networks use. It offers 13 sub-channels, but suffers from congestion

5GHz A radio frequency band for wireless networks. It suffers from less interference than the 2.4GHz band, although range is slightly reduced

802.11a An old wireless networking standard that operates in the 5GHz band, offering headline speeds of up to 125Mbit/s

802.11ac The fastest wireless speed, offering headline speeds of up to 1.3Gbit/s. 802.11ac networks can operate on the 2.4GHz and 5GHz bands simultaneously

802.11g An old wireless networking standard, offering headline speeds of up to 125Mbit/s

802.11n A common wireless networking standard, offering headline speeds of up to 450Mbit/s. 802.11n can operate on both the 2.4GHz and 5GHz bands, although routers that can do both simultaneously are rare

ADSL Asymmetric Digital Subscriber Line: a broadband technology delivered over standard copper telephone lines

AirPlay An Apple technology that lets you beam music and video from one device to another

Bit/s The speed of the network measured in bits per second, where the higher number is the faster speed. One Kbit is 1,000 bits, one Mbit is 1,000Kbits and 1Gbit is 1,000Mbits

DLNA Digital Living Network Alliance: a set of protocols to control the playback of media and how media servers work using UPnP technology (see below)

Ethernet A fast networking technology that requires cables to connect each device. Ethernet comes in two common speeds: 100Mbit/s and 1,000Mbit/s (1Gbit/s)

Fibre A fast broadband technology, slowly replacing ADSL

HomePlug A wired networking standard that lets you use your home's electrical wiring. It comes in several speeds, with 200Mbit/s and 500Mbit/s the most popular

NAS Network Attached Storage: a dedicated storage device that lets you share files and can often act as a media server

SMB Server Message Block: a protocol that lets you share files over a home network

TCP/IP Transmission Control Protocol/Internet Protocol: the language the internet 'speaks'

UPnP Universal Plug and Play: a set of protocols to configure networks automatically, reducing manual intervention

Wi-Fi A standard that ensures wireless networking devices from different manufacturers work together

Wireless router A device that lets you share a single broadband connection with both wired and wireless devices

WPA Wi-Fi Protected Access: a security protocol to prevent unauthorised access of a wireless network. WPA-2 is the latest and most secure version

TL-WR702N

TL-WR710N

TL-WA850RE

Your complete guide to reliable networking

INCREASE WI-FI RANGE

Fed up of not getting a wireless signal? Our guide shows you how to extend range and improve reliability

STREAM MEDIA

View your photos, watch your videos and listen to your music all over your home by following our step-by-step instructions

COMPLETE GUIDE TO INTERNET SECURITY

Find out how to protect your devices from viruses and hackers online. Plus we show you how to recover stolen goods using the internet

SHARE FILES AND PRINTERS

Access all your files and printers from all your devices, saving time, money and effort

INSTALL A NAS

We show you how a network-attached storage device can revolutionise your home network, sharing files and printers, and even acting as a media server

TROUBLESHOOTING

Don't worry if something goes wrong – we're here to help. Just follow our simple guide to find out what the problem is and how to fix it

ISBN 1-78106-254-4
9 781781 062548
£7.99
www.magbooks.com