

Internet SECURITY

complete manual

**1000's
of Must
Have Tips**



Internet SECURITY

complete manual



Viruses, malware, ransomware, phishing, smishing, vishing, social engineering... the list of digital threats with peculiar names expands daily and hardly a moment goes by without some form of attack appearing in the news. We live in interesting times, where data is worth more than oil or gold and your personal information is greatly sought after by cybercriminals, scammers and hackers. How prepared are you for this new age of digital vandalism and theft? Is your computer secure against the continual onslaught of the modern online world? Over this series we'll help you secure your computer, network and devices against such threats and with easy to follow tutorials, help arm you against potential threats and attacks. For parents and guardians, we also cover looking out for your children when online, together with guides on how best to protect them and advice from industry experts. You'll soon be security savvy and prepared for whatever digital threat looms on the horizon.



Contents

Internet Security The Complete Manual



06

Contemporary Security

- 10 Types of Security Risk
- 12 Hackers and You
- 14 Social Engineering
- 16 Ransomware: How it Works
- 18 The Virus Top Ten
- 20 Phishing, Vishing and Smishing
- 22 Pharming
- 24 Windows Security
- 26 Digital Security FAQ

28

Protecting Yourself

- 32 Top Ten Antivirus and Security Packages
- 34 Setting Up Windows Security
- 36 Why Updating is Important
- 38 What to Keep Updated and How
- 40 How to Secure Your Web Browser
- 42 How to Secure Your Home Network
- 44 What are Wireless Security Standards?
- 46 How to Secure Your Wireless Network
- 48 What is Encryption?
- 50 Encrypting Your Windows Laptop
- 52 Top Ten Encryption Tools for Windows
- 54 What is a VPN?
- 56 How Can a VPN Improve Online Security?
- 58 Top Ten VPNs
- 60 Using a VPN for Added Security



62

Online Protection and Recovery

- 64 How Does Information Move Around?
- 66 How Can Internet Data be Intercepted?
- 68 10 Tips to Protect Yourself
- 70 How to Secure Your Devices
- 72 How to Secure Yourself on Facebook
- 74 How to Secure Yourself on Twitter
- 76 How to Secure Yourself on WhatsApp
- 78 What to Avoid when Creating a Password
- 80 Password Generators and Tools
- 82 Top Ten Password Managers
- 84 Shopping Online and Security
- 86 How to Remove a Virus or Malware from a PC







STOP



Over the next
year there is a

69%

CHANCE
you could be
HACKED!

Information regarding cyber security doesn't always have to be technically heavy. In fact, to make it easier to digest, and to just show you how virulent and bitterly hostile computer-borne security threats are, here's a collection of statistics to give you the heebie-jeebies; all the more reason then to keep this manual close to hand.

80% of all cyber crime attacks originate from Russia, China and North Korea

77% of small businesses **don't** regularly back up important data

75% of the health care industry has been infected with malware.*

73% of US citizens have fallen victim to some form of cyber crime

64% of companies have experienced web-based attacks

61% of malicious websites are genuine sites that have been compromised

Social Media Users

50%

Haven't changed
their password in the
last year

20%

Have **never** changed
their password

Sources: Symantec Corporation Threat Report • CSO Cybersecurity Business Report • UK National Cyber Security Centre • Security Intelligence • Hackmageddon.com • UK Office for National Statistics • Bitdefender Labs Report • Herjavec Group

* Figures based on 2017 half yearly report.



A member of
the public is
HACKED every:



Devices hacked in
LESS THAN:



RANSOMWARE
ATTACKS on
BUSINESS every:



250,000
NEW VIRUS
threats
EVERY DAY

GLOBALLY • COST PER PERSON **6 MONTHS***



FIXING
Malware
ATTACKS



LOST
to **Cyber**
CRIME



PAYING
RANSOMS
to remove malware



OVER 3,000,000
REPORTED INSTANCES OF FRAUD
through **cybercrime** against **UK banks** last year





Modern Day Security

The start of the digital age brought with it many advances in the way we work and interact with each other. It's estimated there's 1.2 Zettabytes (1.3 trillion gigabytes) of data available to someone with access to the Internet and whilst most of it may be irrelevant, what's important to you is somewhere within that mass of raw information.

Sadly, the cold hard light of day reveals that with the growth of this voluminous data comes the nefarious acts of those who wish to cause mayhem, panic, theft and other such negative elements. Therefore, as a user you need to make sure that you're protected against the ever increasing digital world of threats, viruses and everything else the Internet has to offer.

This chapter will help you to recognise some of the threats, what they all mean and how they work. We can help you to identify and know what to look out for when online.

10	Types of Security Risk	20	Phishing, Vishing and Smishing
12	Hackers and You	22	Pharming
14	Social Engineering	24	Windows Security
16	Ransomware: How it Works	26	Digital Security FAQ
18	The Virus Top Ten		



Types of Security Risk

There are more security risks for your computer than just the common, run-of-the-mill virus. The amount of digital use the average person has over the course of a week has increased significantly in just a few years, and with it comes a legion of security related issues.

Here Be Dragons

This isn't a definitive list of the possible threats available for the Windows user but here are ten modern risks that you face every time you power up your PC.



Viruses

Viruses have been around for as long as computers. They've moved on from simply displaying the name of the coder on the monitor, a kind of virtual vandalism, and now can disable and wipe the data off a hard drive in mere seconds.



Trojans

The Trojan horse, as the name suggests, is a program that masquerades as a legitimate application but in actual fact contains code that allows a hacker remote access to your computer. Like the legend of the wooden horse the Greeks used to gain access to Troy, once inside your computer it opens and creates an opening for the hacker.



Ransomware

Earlier in the year the UK was gripped in the clutches of the WannaCry ransomware infection. This particular infection exploited a vulnerability in Windows, and quickly spread throughout the NHS and other organisations, locking and encrypting the data on a computer until money was sent to those who unleashed it to the world.



Worms

Although a worm is a type of virus, it behaves differently in that its goal isn't to alter or destroy system files. Rather, it's designed to replicate itself continuously until all the resources and space on the system are consumed. A bit of a nightmare for the system administrator.



Spyware

Spyware invades computers usually through freeware or shareware downloads, which is why you should always download a program from a reputable source. The intent of spyware is to collect information about the user and report it back to those who wrote it.



Adware

Adware is very similar to spyware, in that one of its goals is to monitor the user. However, adware usually goes one step further and bombards the user with Internet pop-up advertising, usually when they open their browser or a new tab. The advertising can be tame, such as gardening equipment, or it can be extremely offensive.



Hacking

While Hollywood would have you visualise the lifestyle of a hacker as something that's quite alluring, in truth it's quite the opposite. The average user is generally under the radar where a hacker is concerned. They're mostly after the corporations, or famous people, but you can have your computer hacked by a neighbour, for example.



Social Engineering

A relatively modern term in the history of computer security, social engineering will have the user deceived into giving away personal information or allowing a scammer into their systems. The recent spate of calls from people claiming to be from the likes of Microsoft or a security firm are a prime example.



Phishing

Much in the same vein as social engineering, phishing is the act of obtaining sensitive information (bank details usually) about a user by being disguised as a trustworthy source. Phishing on social media sites such as Facebook, Twitter, etc. is on the rise.



Rootkits

Rootkits are virus-like programs that are activated before the computer's anti-virus and security suites are started when booting Windows. They can change the way a security suite looks at files, allowing a virus to hide in plain sight and not be detected by the system's security measures.



Hackers and You

We're probably all familiar with the term 'hacker', and what it suggests, but do we really know what a hacker wants from us? More to the point, how are we perceived in the eyes of a hacker? Let's have a look at what the modern hacker wants from the average user.

Being on the end of a successful hack has been likened to having your house robbed. There's a

“
**You've
been
hacked!**
”

feeling of invasion, that someone has rifled through your personal belongings and stolen what's yours.



WARNING

Monetary Motivation

As with most hacks the world over, money is the driving force behind an attack. A hacker will want to enter your system through various means and obtain your bank or credit card details in order to get access to your money. It's plain and simple theft.

Personal Information

Personal information can be extremely valuable to a hacker. Those who manage to obtain information about you, from date of birth, address, social security number and countless other trivial details, can then use your identity to open bank accounts, start a loan and so on. In the end, it is your name that's linked to the fraud.

Parasitic Infection

Sometimes a hacker will use you to get some other target. Perhaps you work at a bank, or something similar, the hacker will then identify you as a target that can be used to transfer a program from your laptop to the work's server. You unwittingly become the carrier of malware, allowing a hacker to gain access to your work.

Exploitation

Exploitation is becoming a common theme among modern hackers. In this scenario a hacker will gain access to your personal information and hold it to ransom. They can then demand anything from money, to more personal acts.

Stealing Bandwidth

Rather than targeting a user purely for financial gain, or something else, a hacker can also want to use your home bandwidth. Generally speaking, the hacker doesn't need to be on the other side of the world, they could be a neighbour who's using your Internet connection to download copyright material.

Access to Your Webcam

Webcam hacking has become more popular in recent years. What happens here is, a hacker manages to gain access to your computer and activates the webcam in order to view what you're doing; and as long as the computer is up and running, they can see everything the webcam can, and they can do so without you even knowing.

Access to Your Microphone

To expand on the previous hack, along with a webcam hack an attacker can also activate a computer or device's microphone. Doing so will allow them to listen in on anything that's being said, so perhaps it's worth covering up your microphone during any future meetings.

Zombie Apocalypse

There are instances whereby you become the target of a larger scale hack. In this case the hacker isn't targeting you specifically, they're simply using your computer as a zombie, a collection of machines connected to the Internet that runs malicious programs against a target. Zombies are often used to conduct DDoS attacks.

Cyber Vandalism

Often you can be the target of an attack that doesn't seem to make any sense. The hacker doesn't want money, they don't want your personal information either. It's just a case of cyber vandalism. Perhaps the hacker wants their name known in the wider world, or just likes to see chaos reign. Who knows why they do it?

Distributing Illegal Material

Finally, a hacker can use your computer as a source or a node for the distribution of illegal material. You won't even be aware of the fact but your computer is successfully trafficking illegal material together with others on the Internet.



Social Engineering

With the rise of wider forms of communication, through social media and so on, comes a new wave of threats called social engineering. There are many forms of social engineering, so let's have a look at what you're up against, and how to combat it.

Social engineering is the new modern way of manipulating people to give up their personal and confidential information. It comes in many guises and under different sub-headings, such as Phishing and the like, but it's essentially all a form of social engineering. Essentially, the scammer will take your human nature and responses and turn it against you for their own gain.

The kind of information the scammer is after does vary, depending on the type of scam being used, but for the most part they're usually after your passwords, bank and credit card details, or login information in order to gain any sort of financial data.

You're probably more familiar with social engineering that you suspect, even if you're new to the term. Recall the emails from someone, usually based in Nigeria, who has come into a fortune in the billions and for some inexplicable reason wants to put the money in your bank account. Needless to say, the money was never there in the first place and should you go through the process you will eventually be persuaded to hand over some banking information which the scammer can then use to steal from you.

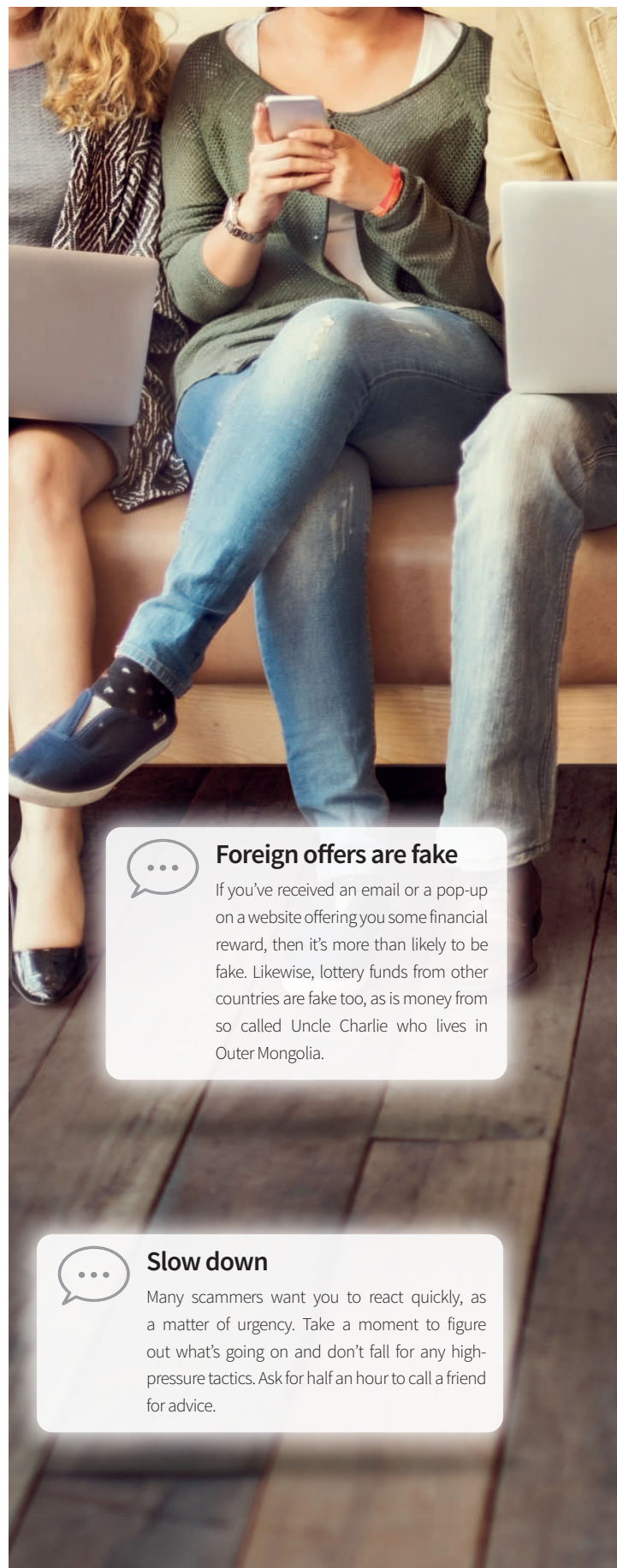
There aren't too many Nigerian scams these days, mostly you get a phone call from someone claiming to be from Microsoft or some other well-known company, who insists that they are tracking a virus or other harmful malware that's currently residing on your computer. They ask you to visit a webpage and download a piece of software that will allow them remote access to your computer. When in, they run a script that displays a wealth of useless information on the screen whilst in the background they run keylogging and hacking software to obtain your online banking details. They can even ask you to log into your bank while connected to make sure everything is working.

Other common social engineering tactics include emails from a friend, who has been hacked, with the scammer masquerading as them. It could be an email claiming to be from your bank, an urgent request for help or someone asking for a donation to a charitable organisation. Be wary, and question everything.

You may think you're not the sort of person to be fooled by a scam but often the

“
**Scam,
scam,
and
more
scam**
”

scammers have employed subtle ways and means in which to bait you.



Foreign offers are fake

If you've received an email or a pop-up on a website offering you some financial reward, then it's more than likely to be fake. Likewise, lottery funds from other countries are fake too, as is money from so called Uncle Charlie who lives in Outer Mongolia.



Slow down

Many scammers want you to react quickly, as a matter of urgency. Take a moment to figure out what's going on and don't fall for any high-pressure tactics. Ask for half an hour to call a friend for advice.



Don't engage

Whilst it's fun to lead a scammer on the other end of the telephone, telling them that the only computer you own is a Commodore 64, it's really not worth it. They know they're scamming, you know they're scamming, so just put the phone down and ignore them.



Research everything

Locate your bank or credit card company's webpage and follow any links to known social engineering scams. Read all the information you can gather about the techniques and tricks used and arm yourself with that knowledge prior to any contact from a scammer. The more you know, the less likely you are to be hoodwinked.



Beware of attachments

Email attachments are an excellent way of distributing malware, viruses and hacking scripts to your computer. If you receive an email claiming to be offering you a deal of a lifetime, and requesting you open the attached file, then it's likely a virus. Research the sender, and best to delete the email.



Never give your password

A bank never asks you for your password, they never call you up or send a text message requesting to enter your password, nor will they ask you for other personal information relating to your account. Treat all requests as suspect and don't give out any of your passwords.



Ransomware:

How it Works

The first instance of an extortion attack is credited to Joseph Popp back in 1989. Since then the frequency, delivery and scale of ransomware attacks has increased significantly; so what is ransomware and how does it work?

Ransomware is a particularly nasty form of malware and digital threat. There's usually some kind of ransomware headlining in the news around the world and those who are the victims are often at a loss as to what to do next.

Essentially, ransomware will infect an individual computer and one of two things can happen: first, it locks the computer, stopping all access to it from the keyboard, then it starts to search for data and encrypt the contents of the hard drive. Lastly it infects the boot sector of the computer and displays a message detailing the type of ransomware and how the individual will pay for the release of the data; the message can even have fake FBI warnings included with it. Alternatively, and the second thing that may happen once a system is infected, the ransomware will lay in wait until a set time and date, then do all of the above and lock the computer. Waiting for a set time will ensure that numerous machines are infected before any fix can be discovered; also if all the infected machines are activated at the same time then there's more of a chance of the attacker getting their ransom paid.

You normally have a set time in which to pay the ransom, usually 72-hours. If the victim doesn't pay in time, the attacker can introduce a second phase into the ransomware code that will either increase the amount demanded or completely destroy the files that are being held at ransom.

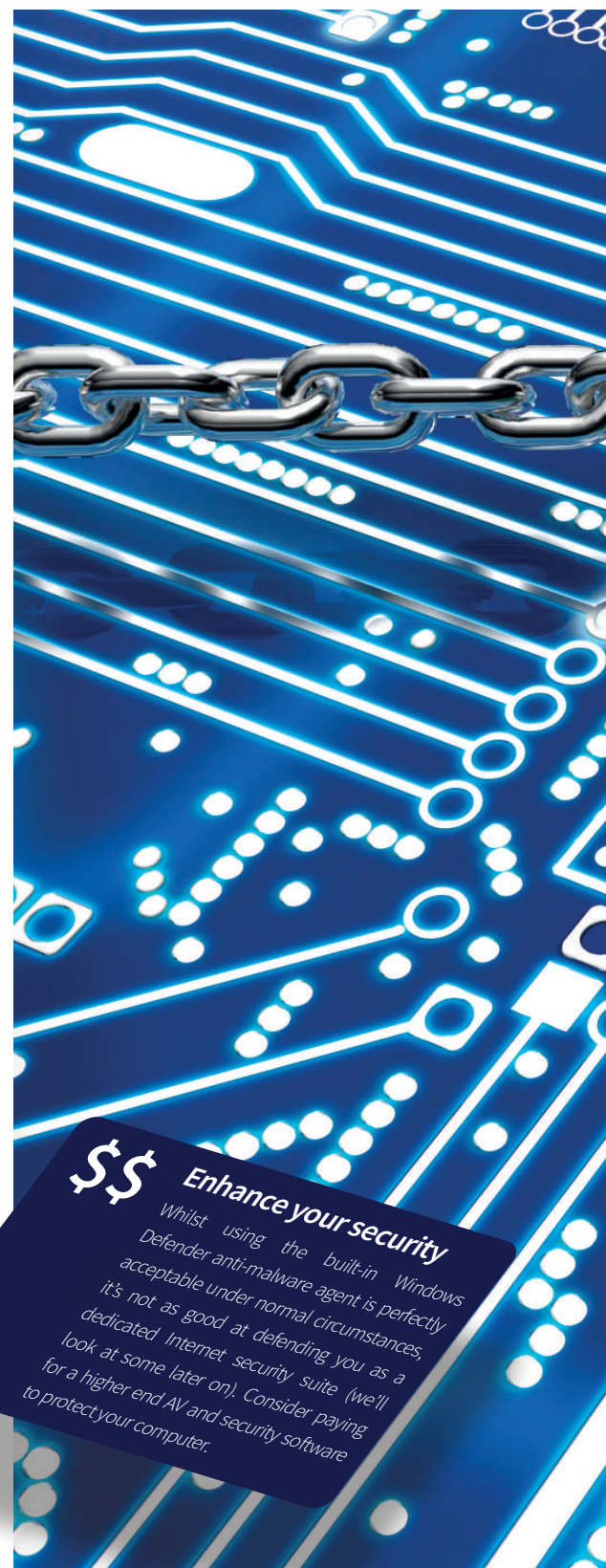
Ransomware can be spread in a number of ways. The more popular choice of delivery is via an infected web page, some form of Flash script that has been hijacked and now contains a link to a remote server where the browser will unwittingly download the ransomware code. More recently there are instances of Drive-by attacks, where the ransomware code locates any USB sticks a user may have in their system and transfer itself in the knowledge that the stick will be inserted into a work's computer.

The WannaCry ransomware attack earlier in the year was by far one of the most prevalent in recent years. It's estimated that more than 250,000 computers across 200 countries were infected, rendering the likes of big companies such as FedEx, Nissan Motor Co and Telefonica SA under siege from its demands. The National Health Service in the UK was hit too, resulting in weeks of chaos and disorder for the staff and patients alike.

How do you avoid getting ransomware on your computer and what happens if you're unlucky

“
What to do
”

enough to be the target of such an attack? Here are some hints and tips for you.



\$\$

Enhance your security

Whilst using the built-in Windows Defender anti-malware agent is perfectly acceptable under normal circumstances, it's not as good at defending you as a dedicated Internet security suite (we'll look at some later on). Consider paying for a higher end AV and security software to protect your computer.



\$\$ Updates

The single most important factor of preventing a ransomware attack is to make sure that your computer has the latest updates applied. Ransomware code usually looks for vulnerabilities and weaknesses in the operating system but if they're up to date and patched, then it's difficult for it to activate.

\$\$ Never insert a random USB stick

If you've found a USB stick somewhere, although the temptation is strong to see what's on it, don't stick it in your computer. Not only could it be infected with all sorts of malware, it could also contain sensitive and confidential data. Either destroy it or hand it over to a security expert at work.

\$\$ Never pay

Your data is locked, and there's nothing that can be done by anyone to save it, so it's really not recommended to pay the ransom. Nine times out of ten, the attacker will take the money and never unlock the data anyway. There's also the threat of more malware being activated after payment.

\$\$ Backup

Set yourself a daily backup schedule, to a USB, cloud or network resource that's separate from your computer. If your data is securely backed up, and you get a ransomware attack, then you can happily wipe your computer, re-install Windows again, then copy the saved data back over.





The Virus Top Ten

Viruses are constantly evolving thanks to more ingenious methods of delivery and due to the developers and hackers tweaking their code to sniff out operating system vulnerabilities. It's difficult to say what the next big virus will be but some scary ones have already appeared on the Internet.

Just to give you an idea of what the future could hold for the computing world,

“

***Digital
Destruction***

”

here are the top ten most destructive viruses unleashed over the last decade into the digital domain.





1 Storm Worm



Storm Worm was released in 2007 and was rumoured to have hailed from Russia. It came in the form of an email link, usually with an important headline to grab the victim's attention. When the victim clicks the link the code is inserted and payload with a backdoor into the system is opened. It infected over 10 million computers worldwide.

2 Conficker



Conficker was a 2008 worm that infected an estimated 15 million Windows computers worldwide. The French Navy, UK Ministry of Defence, hospitals and local police forces were affected. It was spread via Facebook, Skype and mail services, and infected networked computers with a keylogger that the hacker could use to record your keyboard strokes.

3 Daprosy Worm



2009 saw the release of the Daprosy Worm whereby an estimated 20 million computers were infected with a keylogger. What made this such a dangerous virus was that it remained active in Windows Safe Mode, so it was very difficult to remove.

5 Duqu



Duqu was released in 2011 and shared many characteristics with Stuxnet. However, Duqu had different roles: it would work as a keylogger, to steal digital certificates, gather information about an infected PC, or completely wipe the contents of any connected hard drives. Interestingly, parts of the Duqu code were written in an unknown high level programming language.

4 Stuxnet



Stuxnet was rumoured to have been a US Intelligence created virus that was designed to infect Iranian nuclear power plants, thus stopping them from potentially creating weapons grade material. Whether you believe that or not, it was one of the worst viruses to appear in modern times.

6 Shamoon



Shamoon was discovered in 2012 and developed to infect the Windows kernel, the core code of the operating system. It successfully managed to wipe the contents of millions of hard drives and was rumoured to be used in cyber espionage in the energy industry.

7 CryptoLocker



CryptoLocker is a ransomware infection that first appeared in 2013. As with most ransomware code it locks and encrypts your entire hard drive and offers to unlock them if the victim pays up to \$300. Remarkably, the code was able to delete itself whilst still keeping the files encrypted and locked.

8 Regin



2014's Regin virus was spread via fake websites and infected tens of millions of computers. Rumour has it that it was a joint US and UK intelligence created virus for global digital surveillance but we'll leave that for the conspiracy theorists to argue over. Nevertheless, it managed to send information of the victim's computer back to an unknown location.

9 Rombertik's Endless Loop



Rombertik's Endless Loop is an interesting, if somewhat deadly, virus to have sprung up in 2015. When infected, the virus will alter and delete key boot files for Windows computers then force them to reboot. With the boot files missing or altered the Windows PC will continually boot and reboot itself until you re-install the OS.

10 Tiny Banker



Tiny Banker is an information and packet sniffer virus that will record any online banking details the victim enters in their computer. That information is then sent back to several servers which the hackers can then use to access your bank accounts. It's estimated that hundreds of millions were stolen in 2016 thanks to Tiny Banker.



It's tempting to think we've made up the words Phishing, Vishing and Smishing but in actual fact they're all forms of social engineering scams. Whilst we've covered social engineering already, it's worth looking at these three modern day threats individually.

Social engineering, the act of getting information from a person based on their human instinct to react, help or be entrapped into some form of false promise, isn't as modern as the name suggests. Although the term 'social engineering' is in fact relatively new, the process of obtaining sensitive information from a victim has been around for a very long time.

The digital age, of course, has increased the attacks and how they're delivered. No longer is a victim beguiled by post, now they're bombarded by false websites, emails and a string of other cleverly disguised mediums.

Let's break down the three main, modern methods of how a scammer will attempt to obtain your personal and sensitive information: Phishing, Vishing and Smishing.

Social engineering fraud comes in many guises, with oddly sounding names and methods. In the

**“
Gone
Phishing
”**

end, the scammers are after your data, but what do these three in particular mean?

Phishing,

Phishing is the attempt to obtain information from a potential victim through emails, messaging, social media and auction sites. They can come in the form of an email, for example, claiming to have some money available for you or pretending to be from your bank or credit card company. Social media phishing includes individuals befriending you, or pretending to be someone you may know, then asking for information. Similarly a phishing attack can come in the form of a Facebook seemingly friendly test, such as 'name the top five things about yourself and tag ten friends...'. The unwitting victim will happily reveal their date of birth, where they were born, pets names, names of any children and so on. The attackers will gather all that information and use it to their advantage.

Interestingly there are also three different phishing types: Spear,

Clone and Whaling. Spear phishing is designed to specifically target an individual, gathering information such as the above Facebook 'game' whereby the scammer can personalise their attack on the victim.

Clone phishing is an attack type that uses a previously delivered, legitimate email containing an attachment but with the details changed and the attachment swapped for a virus or keylogger. To the victim the email looks real, since it's cloned from a real email, and when the attachment is opened it infects the computer.

Whaling is when a phishing attack targets senior executives of a company or a high-profile individual or business. The attack is a finely crafted email or web address that's created to look business-like and containing information specific to the company or individual. ■





Vishing & Smishing

Vishing is voice phishing, using a telephone call to commit some form of social engineering attack. The victim will, as we've explained previously, receive a call from a legitimate sounding call centre with the person on the line claiming to be from a well-known computer related company. Usually the caller will be led to believe that there's a virus on their computer or that some form of security vulnerability has been detected. The victim will then be guided to a website where the caller can make a remote connection to their computer. Once on the victim's computer, the caller will then run a script that will display reams of data on the screen designed to confuse and baffle the victim. In the

meantime, they're secretly running a keylogger in the background.

In some circumstances they can then claim to have fixed the so called issue but ask you to log into your bank to double-check all is well. With a keylogger in place, they can then see your username and password on their screen; after which they log in and steal from your account.

Alternatively an automated call can ask you to enter your credit card number into the phone's keypad, as it's been reported as being used elsewhere. Of course it hasn't but as soon as you enter the details they're recorded and your card can be used by the scammers. ■

Smishing is an SMS form of phishing. In these cases you receive a text from a seemingly legitimate source, usually your bank or credit card company but also in the form of a competition winner or something free, asking you to confirm your details. There's often a link for you to follow, which leads to a false website that logs your keystrokes and records your data.

Some smishing attacks will ask you to send a return SMS to approve an action, such as a delivery of some goods. The return message is designed to cost significantly more than the usual SMS rate, with the money going straight to the scammers.

One way or another, each of these scams are designed to bait the victim, hence the phishing element, a homophone of the word fishing. The best defence is to ignore, delete or hang up on anything that's even remotely suspicious. Microsoft doesn't know if you have a virus, and nor will it telephone you. Your bank won't email you for your account details and don't be tempted to fill in any Facebook games with personal information. In short, be savvy about baiting techniques and remain vigilant. ■





Pharming

Whilst on the subject of homophones, another recently added word to the long list of security threats is Pharming. Pharming falls within the online fraud layer of security and although in reality it's been around for as long as web pages have, the methods of deception are continually evolving.

So what exactly is pharming? In short, this is the criminal act of producing a fake website and redirecting the victims to it. The website could be anything from a reasonably popular online shopping store, to one of the well-known high street banks. The victim, unaware that the web site is fake, as the front end apes the real thing, even down to the small print at the bottom of the page, will login with their details.

After the user has logged in several options are available to the 'pharmer'. They can collect the username and login details and simply leave the victim with a blank web page; this is usually a method used by an amateur pharmer or those who want a quick username and password grab before disappearing into the darkened corners of the Internet. Otherwise, they can redirect the victim to the real site where they need to enter their login details again. The latter is a more convincing method of pharming, as the victim rarely questions why the bank has asked for their login credentials twice; they often put this down to a mistaken entry on their part.

Either way, the pharmer now has a considerable list of valid usernames and passwords for the bank or online shop they faked, which they can then sell via the Dark Web or use themselves. How do they, the pharmers, get away with being able to do this? Interestingly, there are several ways in which someone can fake a legitimate website.

Pharming has become quite sophisticated in recent years, and with the rise of connected devices that offer Internet

“
Harvesting Time
”

access it's quickly become one of the more popular criminal cyber activities.



⏪ ⏩ x http:// DNS

DNS cache poisoning is the primary method of creating a fake website with the view to setup a pharming scam. This involves the criminal attacking the Internet naming system, which is responsible for creating readable names for websites, such as www.ebay.com and so on, rather than a string of numbers in the form of the IP address, such as www.184.232.124.65 or similar. The Internet naming system relies on DNS servers to provide the conversion between IP addresses and readable web site names. The attacker can mount an attack on the DNS cache, thus changing the way in which traffic moves on the Internet. Effectively, instead of the user's request to go to www.ebay.com, they're taken to the attacker's fake website instead. Thankfully, these kind of attacks generally don't last for long, as the DNS cache is monitored frequently by many different engineers and companies.

⏪ ⏩ x http:// Fake Naming

Fake naming relies on the attacker seconding their pharming attempts with a phishing email. The email can look legitimate and contain relevant information about the person in general. There's often a link at the bottom that although is spelt correctly in the email, is in actual fact a hyperlink to a pharming website that's similar to the real thing but spelt somewhat differently. For example, the email could say 'your overdraft is nearing its limit, please login to www.bank.com to transfer funds...' The www.bank.com part is correct, but the hyperlink and the resulting website may be taking you to www.bnak.com, which although subtly misspelt is often difficult to miss when you're concentrating on the website content.

⏪ ⏩ x http:// Hosts

One method that's more difficult to pull off, though if successful is remarkably effective, is to alter the victim's Hosts file on their computer. The Hosts file is located in C:\Windows\System32\drivers\etc\hosts on Windows computers, /private/etc/hosts on macOS, and /etc/hosts on Linux computers. Its function is to map hostnames to IP addresses, translating the readable websites to IP addresses on a local network. However, it can also be used to circumvent the Internet lookup of a legitimate web site, redirecting you to a fake one. It's not often that the Hosts file can be altered, as it's a system file that requires elevated permission in order to edit, but a cleverly written virus can do the trick.

⏪ ⏩ x Secure | https:// What To Do?

So how can we be prepared for pharming attacks and combat them so we don't become victims?

STEP 1 Always make sure that the website you're visiting is the real one. Double check that the name in the address bar of the browser you're using has the correct spelling and that other elements of the site are correctly positioned and the logo of the site you're at is the most recent.

STEP 2 Never follow a random email's hyperlinks. Most banks will never send a threatening email anyway but if you're tempted to, hover over the link and check that the translated address matches the real web site name of the bank, for example.

STEP 3 Always make sure that you have a good antivirus program installed and that it's up to date. A decent AV will stop any attempts by someone wanting to alter your Hosts file. If possible, you can make a backup of your Hosts file and occasionally restore it if you want to.

STEP 4 Make sure that the web address you're using has the HTTPS protocol before the actual address of the site. HTTPS is the secure version of HTTP, thus providing authentication of the genuine website. In fact, it's a good ideal to always use HTTPS for every site you visit.



Windows Security

Microsoft is often accused of developing insecure and 'broken' operating systems. However, what the Redmond company delivers is an easy to use system that's as secure as it can be without compromising its use. It's a difficult balance to maintain and security can suffer in the long run.

Security leaks, holes and flaws in development code appear all the time, for every operating system. Windows has the bad luck of being

“

**Windows
Security
Improvements**

”

at the top of the security flaw news pile. However, here are ten reasons why it's actually a secure OS to use.





Virtualisation-based Security

VBS is an improvement to the core Windows security, it stands for Virtualisation-based Security and uses a mixture of hardware and software enforced developments to create an isolated, hypervisor restricted subsystem for securing the OS core data. Nothing unsigned by Microsoft is allowed to be injected into the kernel or executed.

Secure Booting

Secure Booting utilises the new UEFI (Unified Extensible Firmware Interface), the replacement for the older and more vulnerable BIOS, along with Windows Trusted Boot code integrity and ELAM (Early Launch Anti-Malware) capabilities, to protect the computer as soon as you power it up.

Windows Hello

Windows Hello may seem like a glamorous feature rather than a security feature but it's really quite an impressive layer of protection. Hello supports passwordless biometric authentication methods, such as iris, facial and fingerprint, together with a PIN code to help protect access to Windows 10.

Microsoft Passport

Windows uses the Microsoft Passport single sign on solution that supports the open FIDO Alliance security authentication standard (www.fidoalliance.org) and utilises cryptographic keys to secure access to network and local resources.

Trusted Platform Module

If your computer has a TPM chip (Trusted Platform Module), Windows can utilise the hardware cryptographic key therein to link Passport and Windows Hello to authenticate the user and operating system with local, network and Internet resources.

Credential Guard

Windows Credential Guard protects the user details and Windows authentication keys within the VBS layer. This isolates the authentication service against network and local attacks, stopping keyloggers and other worms from gaining your login details.

Device Guard

Windows has introduced Device Guard, a highly secure tool that determines which programs and scripts should be allowed to run on the computer. It utilises the VBS layer to protect the core system files and with a list of what's allowed and not allowed to run it can prevent most malicious content from being executed on your system.

Rolling Upgrade

Windows's unique method of upgrades now ensures that the latest versions to software, tools and applications are continually upgraded on the computer. The new rolling upgrade process has been widely criticised by many, as there's no opt-out for upgrades available. On the flip side, you're always up to date.

Windows Defender Security Centre

Windows Defender Security Centre is significantly improved over previous versions of the software. The new Fall Creators Edition version offers virus, ransomware and threat protection, device health, firewall protection, app and browser control and family options all under the one roof.

Protection Features

Among the aforementioned security elements, Windows offers User Account Control, Kerberos Armoring, Smartscreen, TPM Key Attestation, Advanced Auditing Settings, Mandatory Integrity Controls, Virtual Smartcards, EMET enabled protection and many more impressive protection features.



Whilst it's all fine and well learning about the different security risks you face every time you boot up your computer, often questions can go unanswered. We've put together ten popular digital security questions that we hope will help fill in any blanks.

Digital Security FAQ

Understanding Security

Trying to understand the digital security world can be hard work. There's so much to take in, that it's easy to become lost in the quagmire of acronyms and homophones. Hopefully we can help you out with these ten FAQs.



“

Do I need an antivirus program?

”

Without a doubt, yes. Windows uses the built-in Windows Defender program to help protect you online. It's more than ample for most users but often better security is required.

“

Does having extra security cost?

”

Most of the security changes you can adopt don't cost anything, just you being more aware and knowledgeable about what's going on. In terms of an antivirus product, most of the better total security suites will cost you an annual subscription.

“

Viruses and malware are only on dodgy sites, right?

”

No, sorry. Even legitimate websites can be infected with a virus or some other form of malware. Remember too, a computer virus can enter your system in other ways, not just online.

“

How often do I need to update everything?

”

Windows keeps a continual update cycle in operation, delivering the latest updates in the background. However, it's always best to do a daily check for any updates for both Windows and any programs you regularly use.

“

Is online banking safe?

”

Online banking is remarkably safe and utilises the latest and continually evolving security encryption methodologies. There's military grade security at every level of the online process, and it's highly unlikely to be hacked.

“

How do I know if something being offered is a scam?

”

That's a difficult question to answer. More often than not, if it's too good to be true then it's likely to be a scam of some form or another. There are times though when genuine offers are made. It's best to research as much as possible before committing to anything.

“

Are hackers after me?

”

Whilst it's true that most hackers aren't interested in the average user, they're after bigger targets, there are instances where you could be targeted for one reason or another. Generally speaking, the average user will only be targeted en masse in a country-wide phishing or similar attack.

“

I think I've just been scammed, what do I do?

”

If you think you've been scammed, you need to quickly make some changes: change your Windows password, inform your bank that your details may be compromised, email friends and relatives that you've been scammed, file a police report, scan your computer for threats and check your credit card reports.

“

Can I keep a phishing phone scammer on the line?

”

Yes, there's nothing stopping you. A school of thought is that while you keep them on the line, turning it into a mock-prank call, you're saving someone else from being duped. However, it's best to simply tell them you know they're trying to scam you and hang up.

“

I've opened a scam email attachment, what do I do now?

”

There's a good chance you may have a virus on your computer. Close all open programs, open Windows Defender and do a Full Scan of the system. If anything is detected Defender will tell you what to do. Then, consider a third-party AV suite and scan the computer again.





Protecting Yourself

Being able to recognise a scam or virus is one thing but you need to know how to protect yourself against possible attacks. We look at the top Internet security packages, from Bitdefender, Kaspersky and McAfee, as well as what encryption is and how to make it work for you.

Using a Virtual Private Network is an excellent way to improve your Windows security, we'll look at how a VPN works, what the best VPNs are and how to install and use one on your PC.

30	Be Smart	50	Encrypting Your Windows Laptop
32	Top Ten Antivirus and Security Packages	52	Top Ten Encryption Tools for Windows
34	Setting Up Windows Security	54	What is a VPN?
36	Why Updating is Important	56	How Can a VPN Improve Online Security?
38	What to Keep Updated and How	58	Top Ten VPNs
40	How to Secure Your Web Browser	60	Using a VPN for Added Security and Privacy
42	How to Secure Your Home Network		
44	What are Wireless Security Standards?		
46	How to Secure Your Wireless Network		
48	What is Encryption?		



Be Smart

We've looked at some of the many varied ways in which you can be compromised by a digital attacker and some of the ways in which you can help protect yourself. However, it's often more beneficial to be able to recognise the signs of a digital security issue.

Weakest Links

In terms of digital security, you're only as strong as the weakest link in your security chain. You can tick all the security boxes but if you don't know what to look for in the first place you're still vulnerable.

PASSWORD CHANGE

A good sign of a breach in your digital security is the sudden changing of a password. It can be for a random site, webmail or just something small to begin with. Sometimes a hacker with a keylogger in place will test the water before accessing your bank, in which case you need to virus scan your PC immediately.



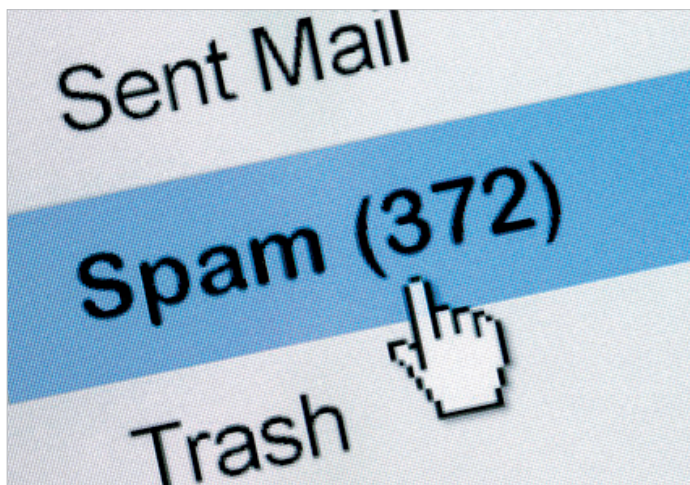
BANK ACTIVITY

If you check your bank activity regularly and you've noticed some odd, small transactions that you fail to identify, then your account could already be hacked. Sometimes hackers will take small amounts or purchase inexpensive items to check the validity of an account before emptying the vault as it were. Contact your bank immediately.

Search your statement					
< Dec 2016 Jan Feb > All transactions					
All Transactions					
DATE	DESCRIPTION	TYPE	IN (£)	OUT (£)	BALANCE (£)
View Pending Transactions					
22 Feb 17	SAVE THE CHANGE	BP		0.30	125.00
21 Feb 17	OASIS DENTAL CARE	DEB		19.70	125.30
20 Feb 17	NEXT DIRECTORY CAT	FPO		40.00	145.00
20 Feb 17	J SLOCOMBE	TFR	40.00		185.00
20 Feb 17	D M CUMMINGS	FPO		55.00	145.00
Load more transactions					

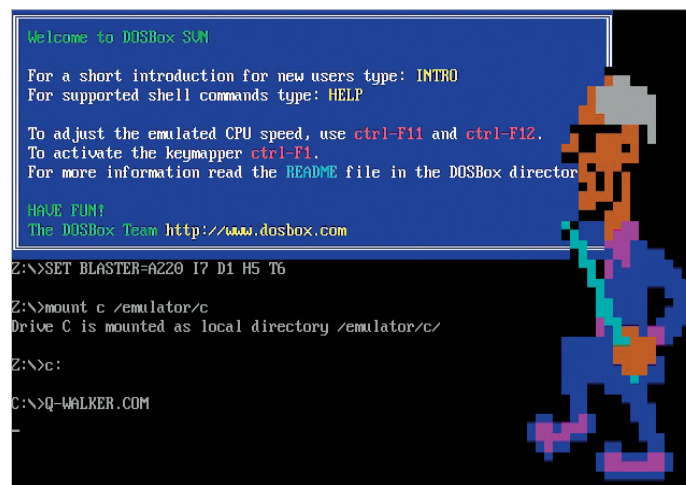
PERSONAL SPAM

We all receive spam emails of some form or another. However, if you suddenly start getting emails of a more personal nature, then you need to look at where that information could be coming from. The details could be your full name, date of birth, knowledge of any children or even a recent accident you may have been involved with.



SLOW PC

One of the many signs of your computer being infected by a virus is the sudden slowing down of the overall system. Most operating systems, Windows in particular, slow down over time but if you power up your computer one day and it's noticeably slower than usual we'd recommend you run a virus scan.





Top Ten Antivirus and Security Packages

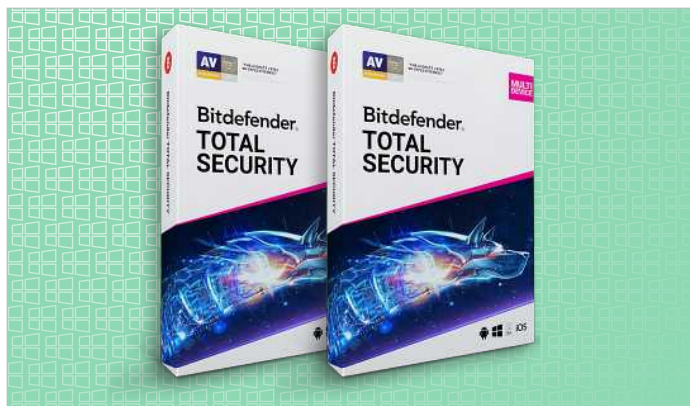
While the built-in Windows Defender is a great antivirus and security tool, it's nowhere near as capable as one of the many third-party security suites. The likes of Bitdefender, McAfee and Symantec have years of security specialism behind their products.

Better Protection

A third-party security suite offers much more than virus scanning. With one of these, you're covered against most, if not all, digital threats. Here are ten security suites worth considering if you're serious about your digital protection.

BITDEFENDER

Bitdefender Total Security security suite from one of the world's leading security specialists. This version offers unrivalled levels of protection and performance for Windows, macOS and Android platforms. There's even an advanced ransomware protection element to help protect your folders.



SYMANTEC

Norton Security Premium is Symantec's top choice for the home user. With it, you can protect up to ten PCs, Macs, smartphones, or tablets and it'll keep you safe when shopping online, general surfing, or when conducting transactions.



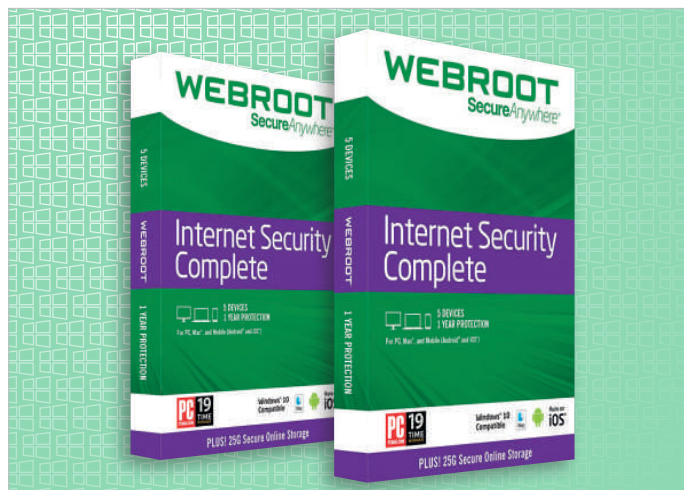
MCAFFEE

McAfee Total Protection offers a 100% guarantee of virus removal, or you get your money back. There are three main versions available: Antivirus Plus, Total Protection and Livesafe, each has its own particular twist, but all offer excellent security features and benefits.



WEBROOT

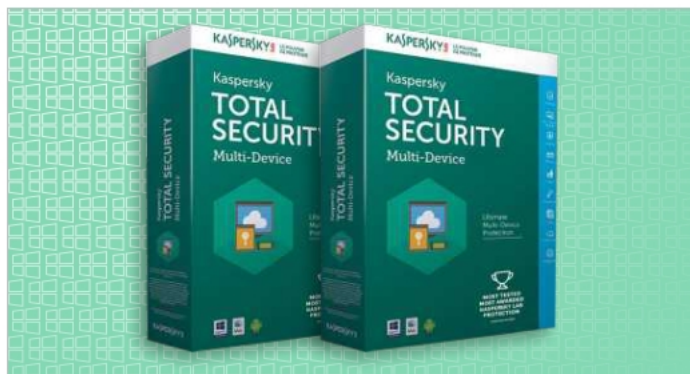
Out of the three possible solutions available from Webroot, Webroot Internet Security Complete is the one to consider for home users. With it, you're protected from virtually any threat, as well as offering 25GB of secure online cloud storage.





KASPERSKY

Kaspersky's Total Security is one of the best go-to products available on the market. It's great value for money and offers superb protection for your PC and other devices. You get parental controls, secure password storage, encryption and identity protection all under a single security suite.



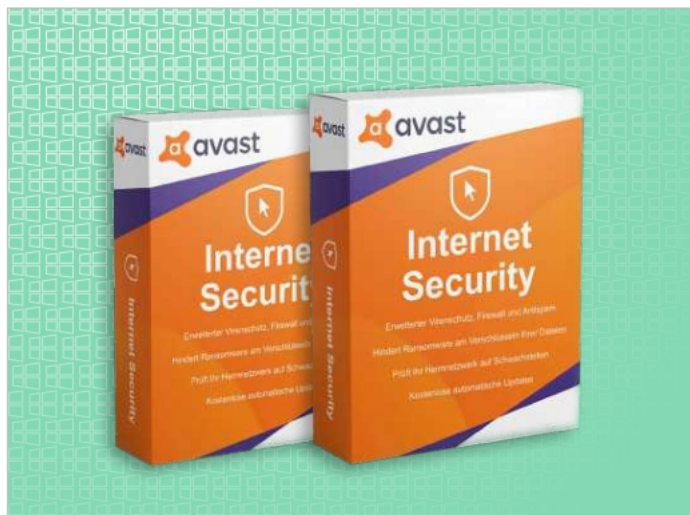
ESET

ESET Internet/Cyber Security is a comprehensive protection package for everyday users. It offers online banking protection, alerts for any malicious attempts to control your webcam and a fine-tuned balance between security and privacy.



AVAST

Avast has offered free antivirus software for many years, but its other products: Internet Security and Premier, are also well worth looking into. With both versions, you'll get online banking protection, identity protection and email protection, all for a reasonable cost too.



F-SECURE

F-Secure has been in the security and protection business for a lot of years and as such, its products are often considered one of the best available. F-Secure Total is the top choice for the home user, as not only does it provide superb antivirus protection, it also offers a Virtual Private Network (VPN) for added privacy when online.



EMSIOSOFT

Emsisoft Internet Security is an award-winning security suite that offers plenty of great features and elements. It's quick, easy to use, cost effective and does an excellent job at protection you and your devices from modern security threats.



TREND MICRO

Trend Micro Maximum Security offers superlative protection for up to five different devices along with extended protection for children, Internet passwords and privacy on social media sites. It's great value for money and performs excellently too.



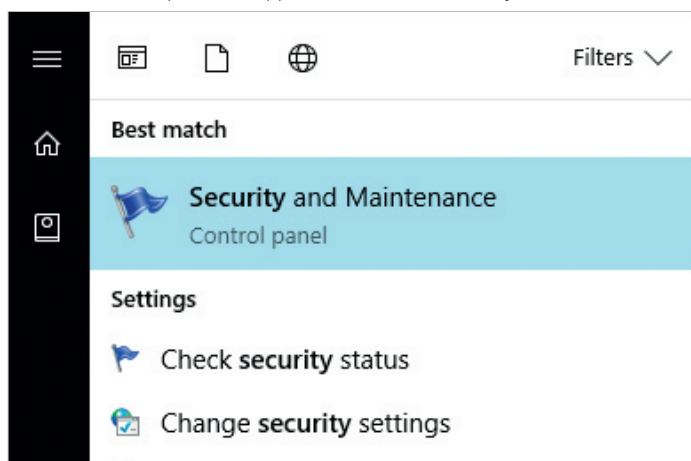
Setting Up Windows Security

Before we dig deeper into the many levels of Windows security features, it's worth taking a moment to check that the initial security features are in indeed up and running, and doing what they're supposed to.

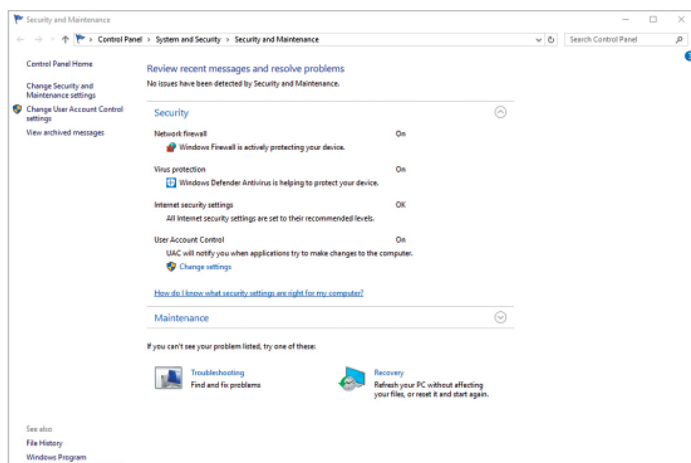
Are You Secure?

Remarkably, despite having an antivirus client installed, some users aren't even aware of the default Windows security features. Here's a quick ten step process to check everything is working as it should.

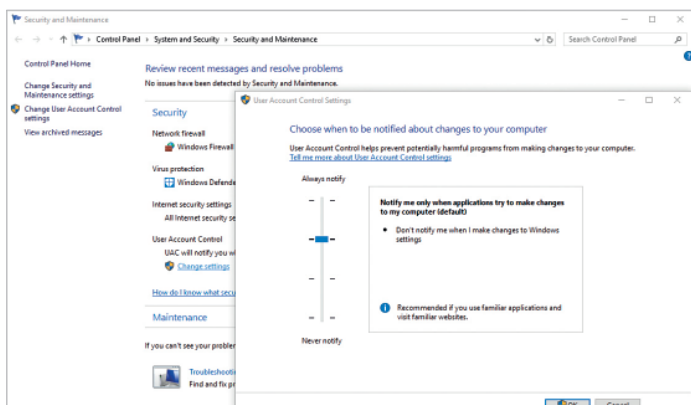
STEP 1 Start by clicking on the Windows Start Button or pressing the Windows key on your keyboard. Enter security into the search bar and click the first option that appears in the results, Security and Maintenance.



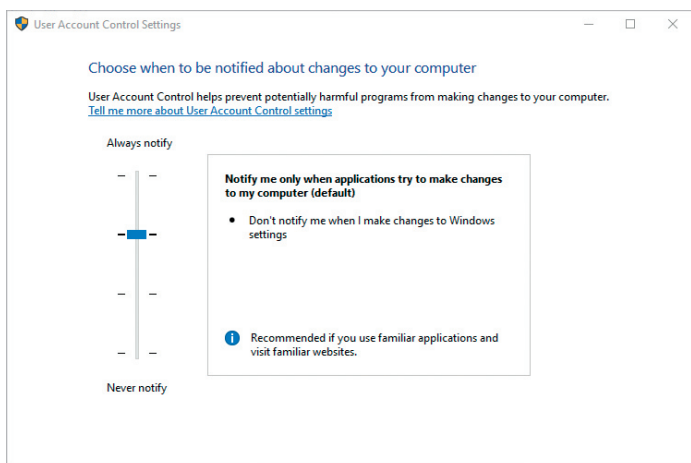
STEP 2 This will open the Security and Maintenance section of the Control Panel. There are two main sections within this page, click on the Security section to expand it. Ideally all the options within the Security section should be displaying On, with the exception of Internet Security Settings which will display OK.



STEP 3 Should any of the options display No, then you'll need to check the setting relating to that particular feature. For example, if your User Account Control (UAC) is set to Off, click the Change Settings link under the UAC option. The other features can be found via a search from the Windows Start Button.

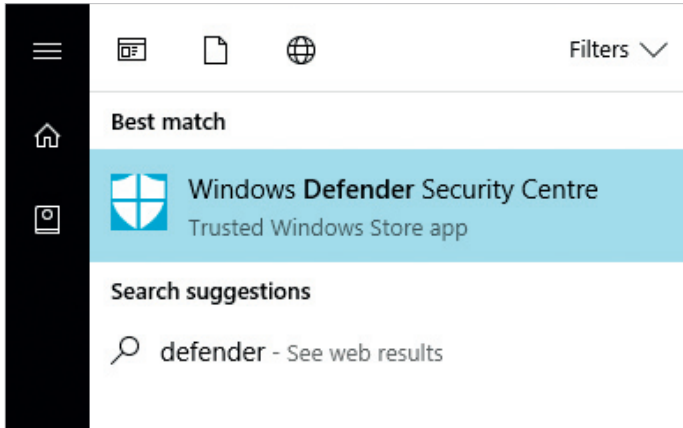


STEP 4 UAC will warn you of any attempt to access a system critical file. If any malware wants to alter a file, then you're asked if you want to proceed; obviously you don't, so you can say no and investigate the issue. There are various settings to choose from but the second step down from the top is the recommended.

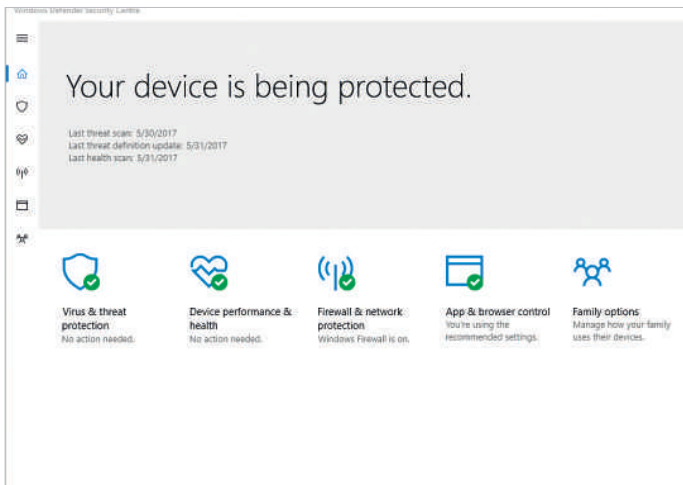




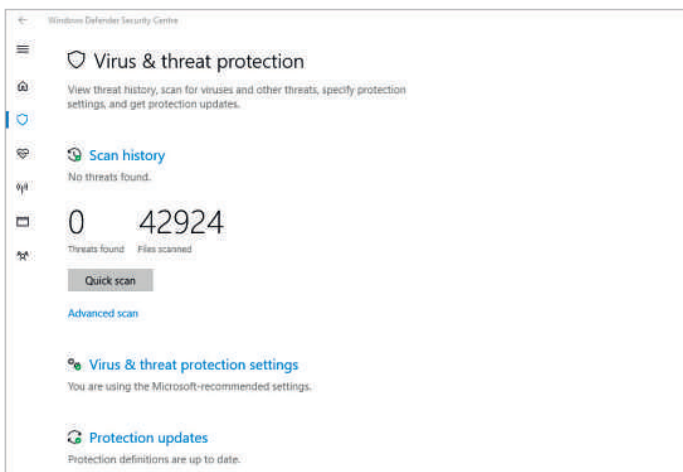
STEP 5 Close down the Security and Maintenance window, then click the Windows Start Button and search for Defender. Click the resulting Windows Defender Security Centre option.



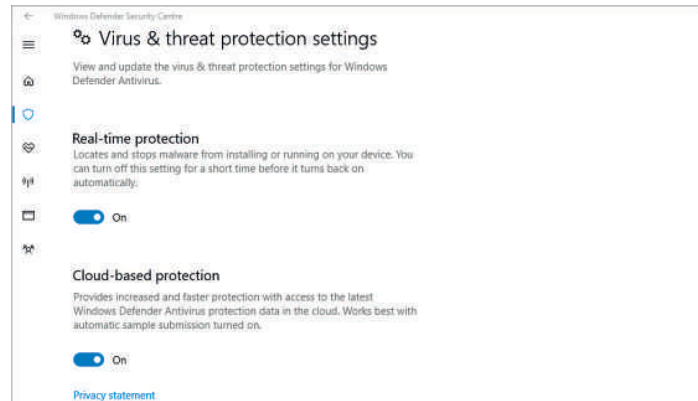
STEP 6 If you're not using a third-party security and AV suite, then you need to make sure that Windows Defender is activated and working. There are numerous options available in the new-look Creators Edition Windows update of Defender. Each can be selected with a mouse click and viewed separately.



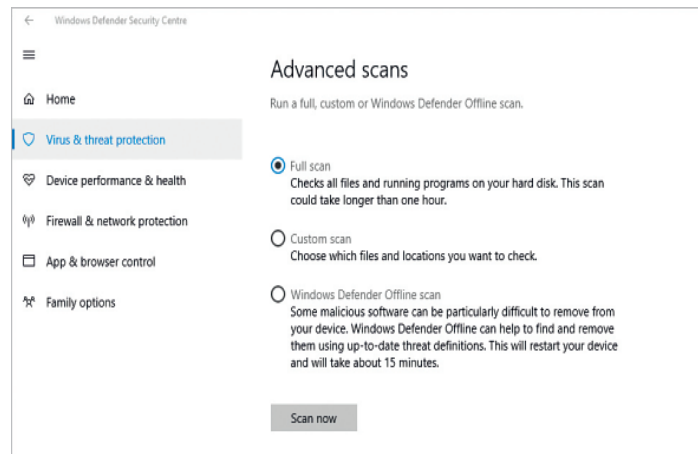
STEP 7 Click the Virus & Threat Protection option. This will open a new window allowing you to perform a Quick or Full Scan of the system that details the number of threats found and the number of files scanned.



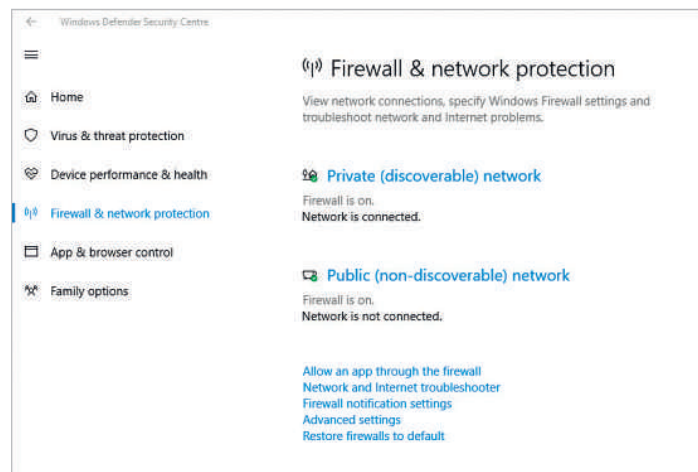
STEP 8 If you click the Virus & Threat Protection Settings option, you can further opt to improve the system protection. Make sure that all the sub-options are set to On and scroll down to define the program's default Notifications.



STEP 9 Returning to the main Virus & Threat Protection page, you can click the shield icon from the strip to the left of the screen; then click on the Advanced Scan link, located under the Quick Scan button. Within are options to run a Full System scan, a Custom scan (of a network location, for example) or an Offline scan.



STEP 10 Lastly, click on the Firewall & Network Protection from the icon strip to the left. Again, if you're not using a dedicated, third-party security suite, make sure that the Private and Public Firewalls are set to on, thus protecting your system from unwanted intrusion.





Why Updating is Important

Continual updates, rebooting after an update has been installed, then the inevitable second reboot straight after the first to apply the update: it's little wonder people stray from the regular update checks. Whilst it can be a pain though, keeping things up to date is a top priority.

Update, reboot, update, reboot

Updates may well be the bane of the modern computer user but they are there for a reason. It's not the 8-bit era anymore, we need those updates to help protect our security. Here are 10 reasons why they're important.

PATCH VULNERABILITIES

Windows updates patch recognised security holes in the core system. Many of the viruses around today exploit a vulnerability in the Windows code that hasn't been fixed yet. So when an update comes along, that potential flaw will be ironed out.



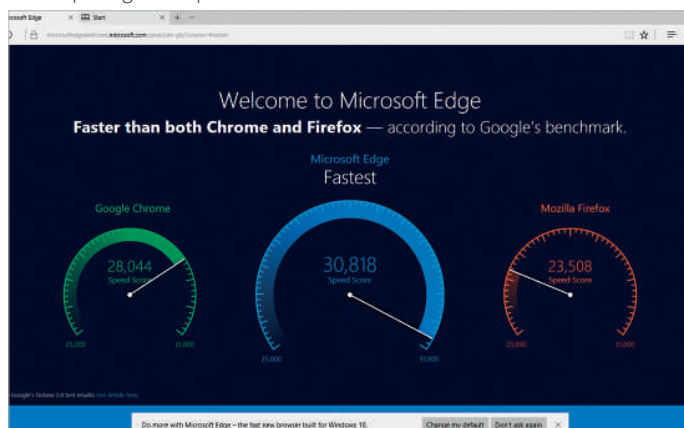
EXTRA SECURITY

In addition to potential security glitches in the code, often an update can contain an extra level of security that's been programmed in by the developers. For example, the code that handles remote desktop requests has had a security patch but another code that handles the authentication is hardened as a result.



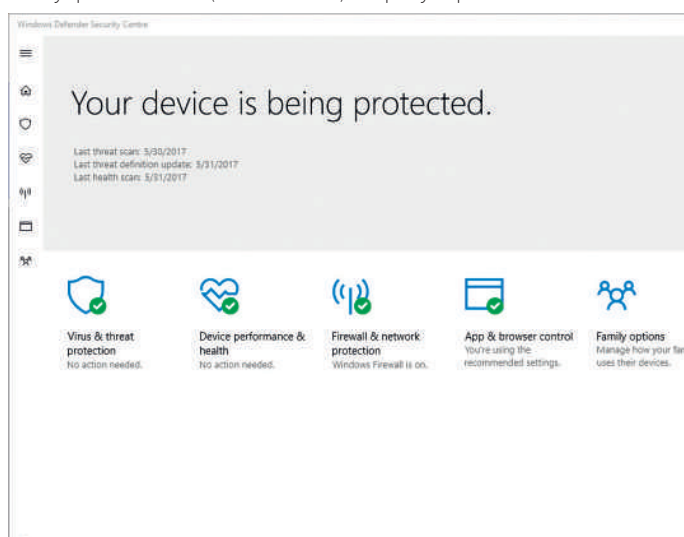
BROWSER UPDATES

Windows comes with many different programs to make it a more appealing environment. They include Internet Explorer and Edge browsers. As a part of Microsoft, these will need to be in tip-top working order to help prevent any modern Internet-borne viruses from entering the system. Daily update checks will keep things in shape.



DEFENDER UPDATES

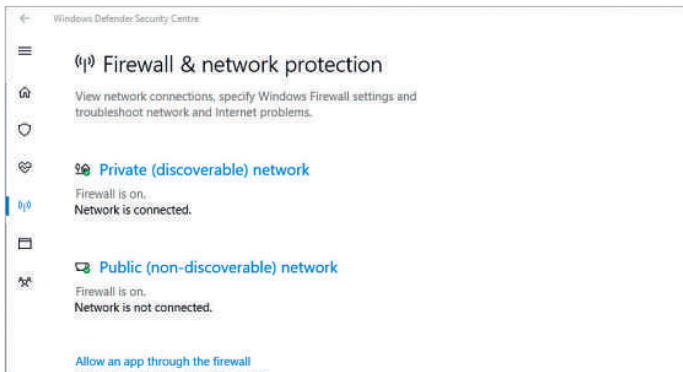
Windows Defender and its other security elements will require at least one update a day to keep up with the latest virus definitions. This is a much needed aspect of updating, as even if you only go online once every so often, being protected from locally spread malware (USB drives etc.) is equally important.





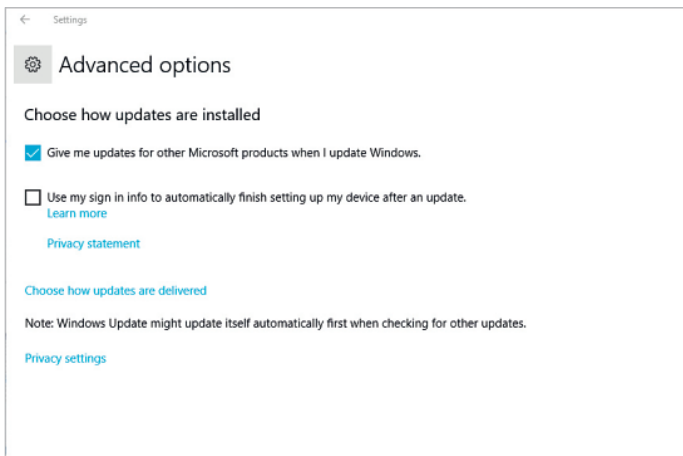
FIREWALL UPDATES

To expand the last reason, the Windows Firewall is one of the first layers of security on your system. With it, access to your computer from another source is monitored and even blocked, stopping potential threats before they even hit the virus defence layer. Updates make sure that the Firewall is up to scratch for the job.



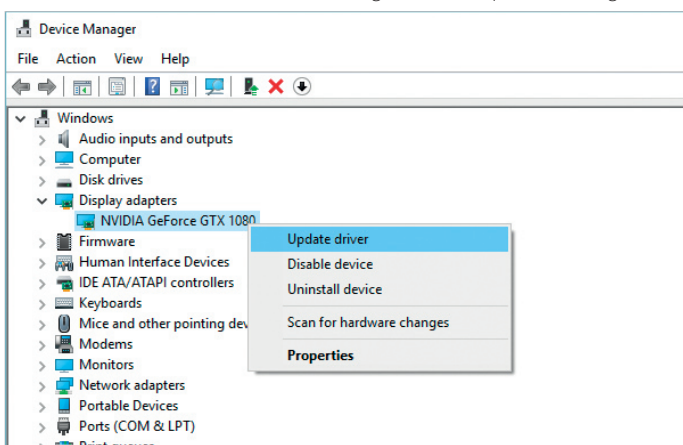
OFFICE PATCHING

It's not just the Windows core files that require regular updates, if you use Microsoft Office that can be a part of the overall Windows update schedule. There are vulnerabilities in Office too, which when exploited can allow malicious code in the system. Tick the Give me updates for other Microsoft products box in Windows Update's Advanced Options.



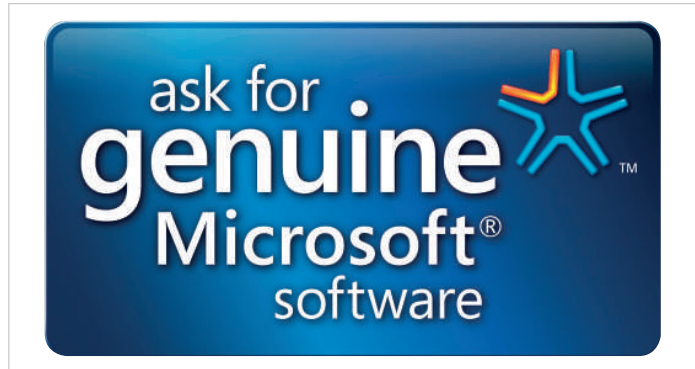
SIGNED DRIVERS

As well as Office, Microsoft provides base-level drivers for most of the hardware available today. These drivers are signed and verified as safe, so any new piece of hardware installed will work and will be safe according to the driver protection engine.



GENUINE SOFTWARE

Non-genuine copies of Windows have been a thorn in Microsoft's side since illegal file sharing on the Internet gained popularity. These days the act of downloading something illegal is rampant. Windows updates ensure that you're using a genuine copy of the OS, which will ultimately secure you PC against threats from pirated copies.



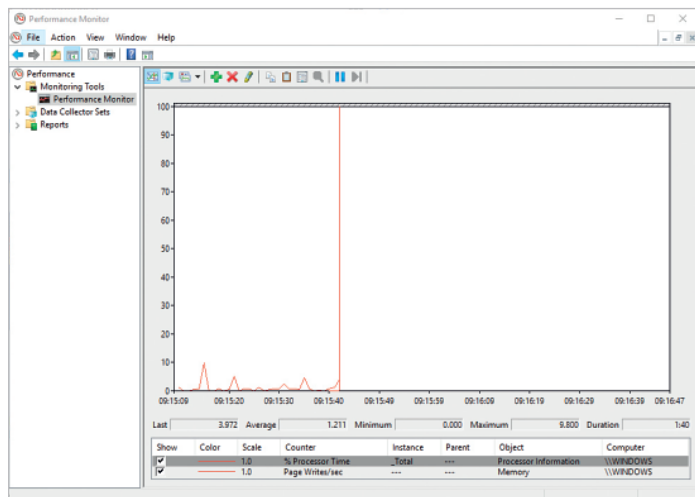
FUTURE UPDATING

Microsoft has big plans for the future of Windows, it's often mentioned that this will be the last full version of the OS as they will be running Windows as a service as opposed to different versions over time. This means it will be a constant update cycle with adding or removing of features. Updates ensure you're running the latest versions.



STREAMLINING CODE

Updates not only patch any vulnerability, they can also free up system resources by improving the code and streamlining the available resources. In short, if your computer is performing better, then it can easily handle background virus and threat scans without affecting what you're doing.





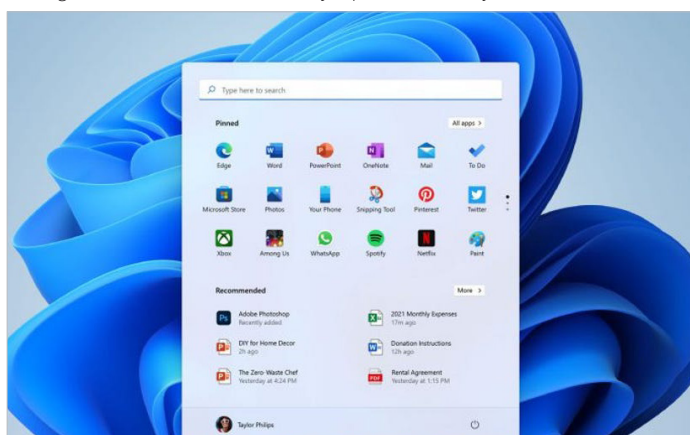
What to Keep Updated and How

Discussing updates is one thing but how do you go about making sure that you have the latest updates and that all the necessary components are being updated correctly? Thanks to the improved update process of Windows, this is surprisingly easy.

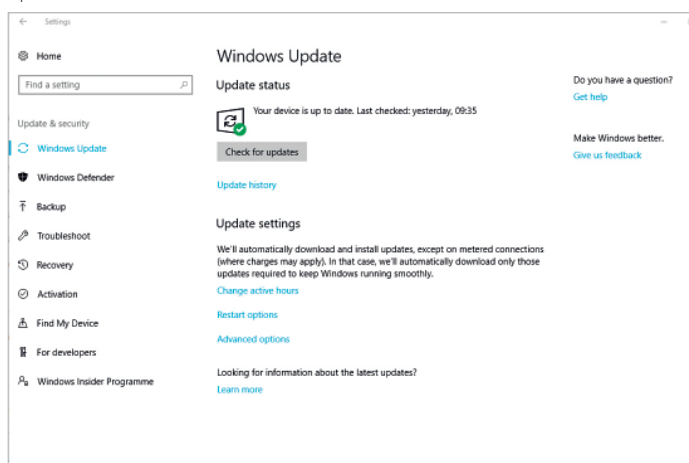
Keeping Up To Date

Whilst it's easy to update Windows, there are elements that can be missed. We've already mentioned that it's not only Windows that needs updating but also software and drivers.

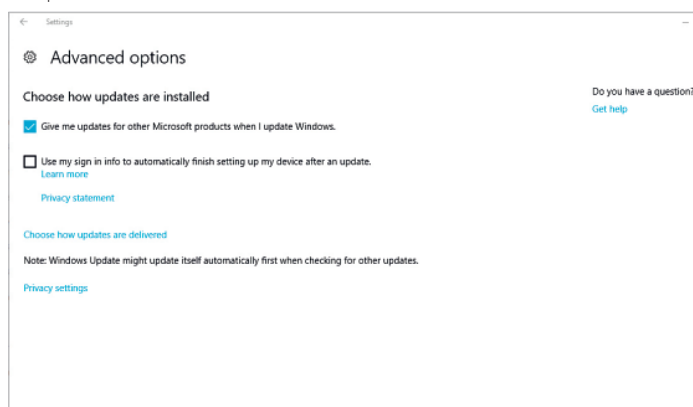
STEP 1 The first port of call is undoubtedly Windows Update. Click on the Windows Start button followed by Settings, the cog icon just above the power icon on the strip to the side. This will open the Windows Settings interface, locate the last entry, Update & Security and click it.



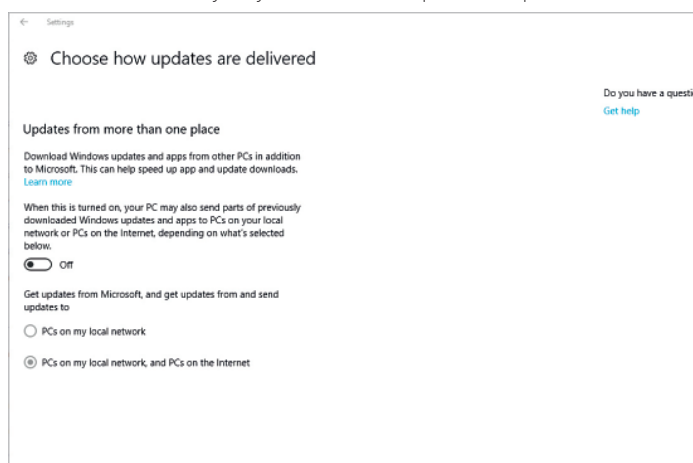
STEP 2 By default Windows Update will automatically check for, download and install updates for the core Windows files. You can check for any on the spot by clicking the Check for updates button; and you can see what's already been updated by clicking the Update history link under the update button.



STEP 3 If you click on the Advanced Options link under the Update Settings section, you can then tick a box that enables Windows to automatically check for updates for other Microsoft products, such as Office and so on. It's recommended to make sure the box is ticked, for better security and protection.



STEP 4 Within the Advanced Options page click the link for Choose how updates are delivered. This page details the way Windows updates can be pushed to other computers on your network, or even the Internet. Whilst it's a grand idea, there are concerns over privacy from some factors of the community. It's your choice but we prefer this option is Off.

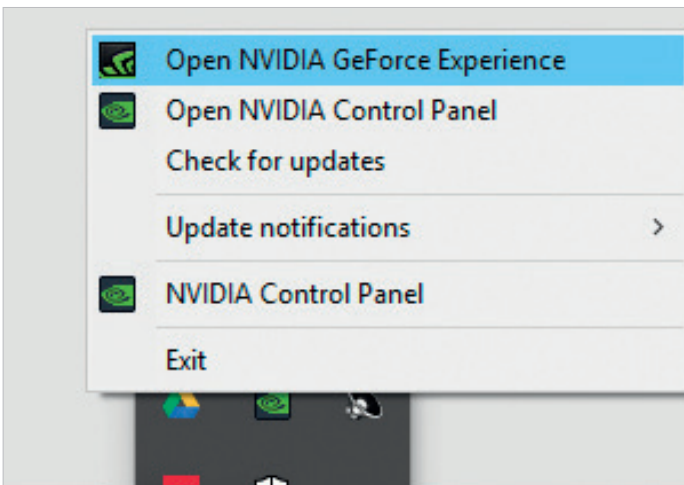


**STEP 5**

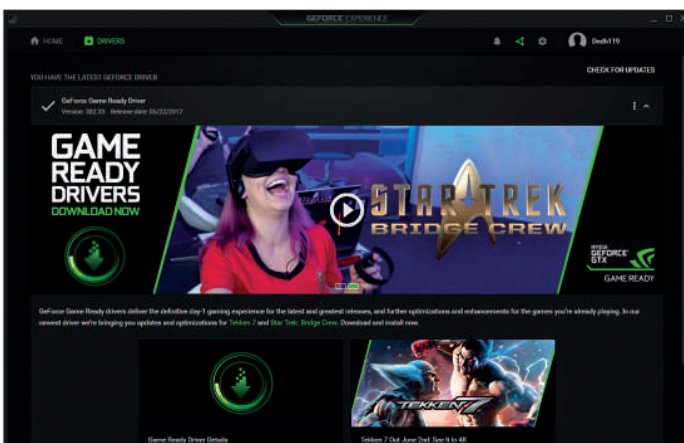
Hardware drivers are usually automatically updated by Windows Update but whilst signed by Microsoft the drivers themselves aren't always the latest versions. Therein lies a problem: even though signed, the MS drivers won't utilise the hardware as well as the driver developed by the hardware manufacturer.

**STEP 6**

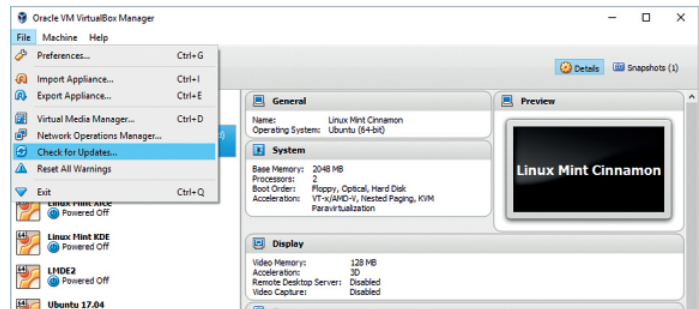
In such cases it's often best to use the hardware manufacturer's driver, as this is more up to date and features security patches as well as performance updates. For example, if you own an Nvidia graphics card right-click the Nvidia icon in the taskbar and select Open Nvidia GeForce Experience.

**STEP 7**

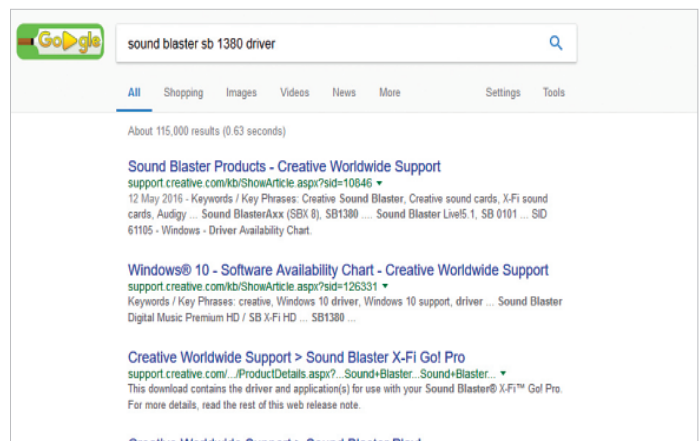
The Nvidia GeForce Experience allows you to improve in-game graphics and check for the latest drivers. Usually this is done automatically, and you are notified of any available drivers. However, if you want to check manually, click on the Drivers tab followed by Check for Updates.

**STEP 8**

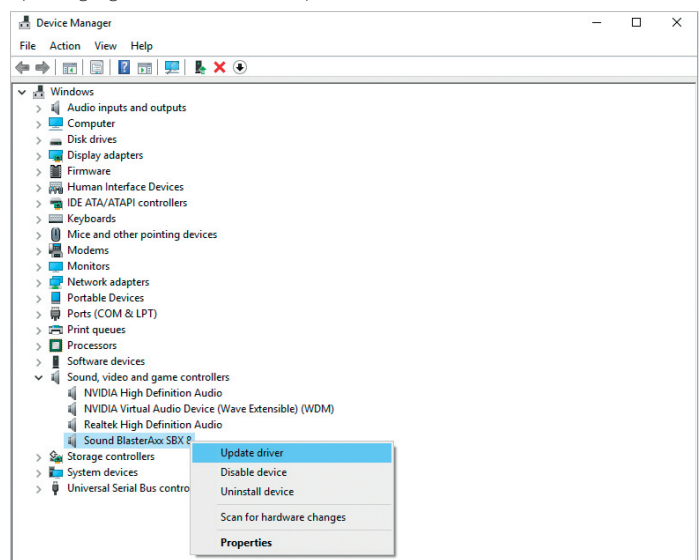
Third-party programs and applications also require regular update checks. Again, this is usually done automatically; when you launch the program in question it often checks for the latest version. If not, look for links such as Check for Updates or similar, usually in the Help, About or even under the File menus of your favourite app.

**STEP 9**

If you've attached some hardware and Windows hasn't been able to load a driver for it, and there isn't any documentation detailing the driver (this often happens with hardware purchased from eBay and the like), then you'll need to hunt one down. Start by locating the device's product name and number and enter it into a search engine.

**STEP 10**

You can often force Windows to locate a driver by right-clicking the Windows Start button and choosing Device Manager from the menu. In the Device Manager window, select the hardware you want updating, right-click it and select Update Driver.





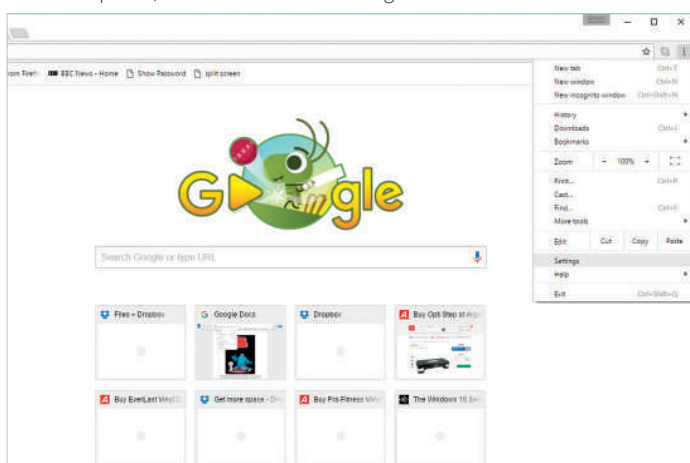
How to Secure Your Web Browser

The web browser is possibly the weakest link in the entire security chain. It's the software product that's on the front line, the one that will inevitably bear the brunt of any Internet attacks and as such, attackers focus a lot of effort on making the browser a portal into your system.

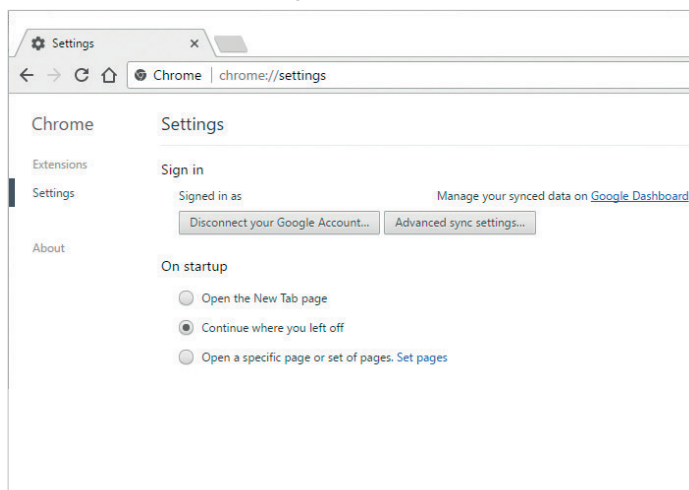
Safer Surfing

Securing your web browser isn't too difficult. There are plenty of options available, including some third-party add-ons you can use to improve security. For this tutorial, we're using Chrome.

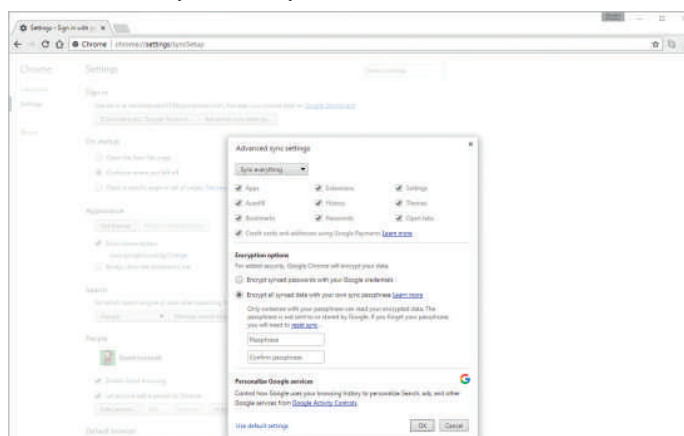
STEP 1 Start by opening Chrome and clicking on the three vertical dots in the top right of the browser window. This is the link to the available options; from the list choose Settings.



STEP 2 It's generally recommended that you sign into Chrome using a Google account, as this can greatly improve the overall security of the browser. For example, when you sign in, under the Sign In section in Settings, click on the Advanced Sync Settings button, the first option available.



STEP 3 With the Advanced Sync Settings box open, select the option for Encrypt all synced data with your own sync passphrase. Enter a secure passphrase you can remember in the boxes provided and this will enhance the security of all data synced between Chrome and the Internet.



STEP 4 Look to the bottom of the Settings page and click the link for Show Advanced Settings. The first new section to appear under the Advanced settings is Privacy. Start by clicking on the Content Settings button.

Privacy

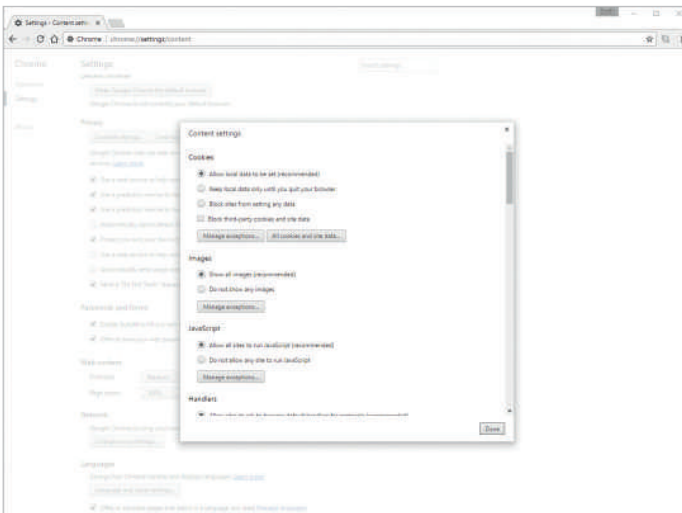
[Content settings...](#) [Clear browsing data...](#)

Google Chrome may use web services to improve your browsing experience. You may opt out of these services. [Learn more](#)

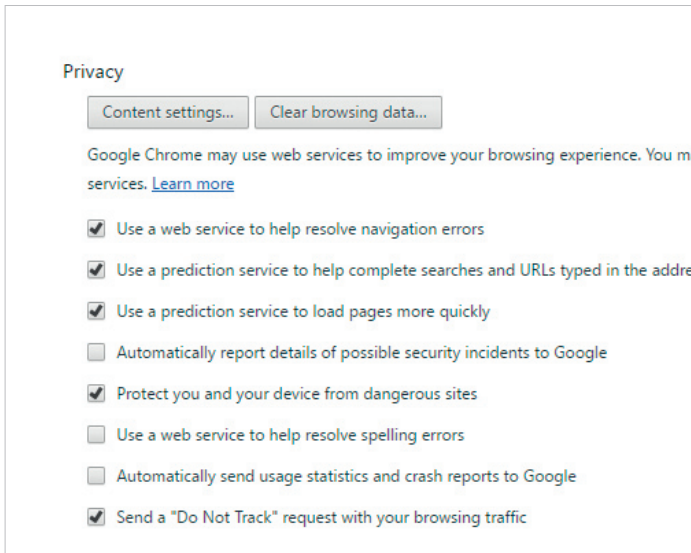
- ☒ Use a web service to help resolve navigation errors
- ☒ Use a prediction service to help complete searches and URLs typed in the address bar
- ☒ Use a prediction service to load pages more quickly
- ☐ Automatically report details of possible security incidents to Google
- ☒ Protect you and your device from dangerous sites
- ☐ Use a web service to help resolve spelling errors
- ☐ Automatically send usage statistics and crash reports to Google
- ☒ Send a "Do Not Track" request with your browsing traffic



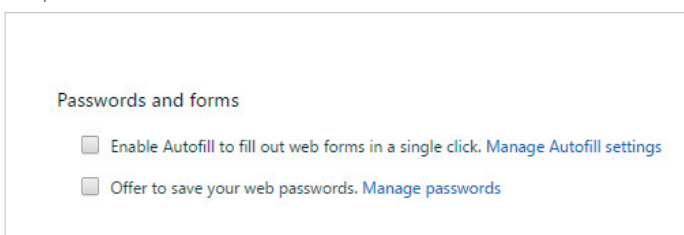
STEP 5 Content Settings allows a greater degree of control over Cookies, JavaScript, Flash, Pop-ups, your computer's microphone and even the webcam. It's an extensive list so we can't go into all the options within this limited space. For maximum security, disable JavaScript and Flash and make sure the mic and webcam are protected too.



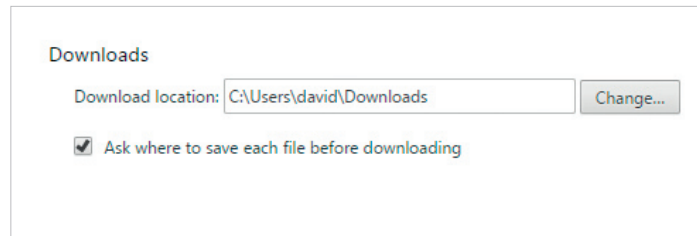
STEP 6 Click the Done button when you're finished with Content Settings, to return you to the Chrome Settings page. Within Privacy still, ensure the last option, Send a "Do Not Track" request, is ticked. This will stop any tracking elements from monitoring your browsing activities.



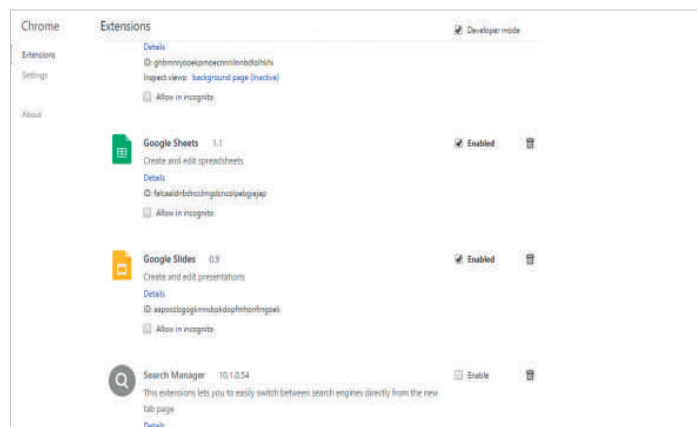
STEP 7 Just under the previous step's tick box, it's also recommended to untick the two Passwords and Forms boxes that offer to enable Autofill and Save your Passwords. Whilst it's a pain to constantly enter passwords, this will stop any hijack Chrome attacks from gaining your usernames and passwords.



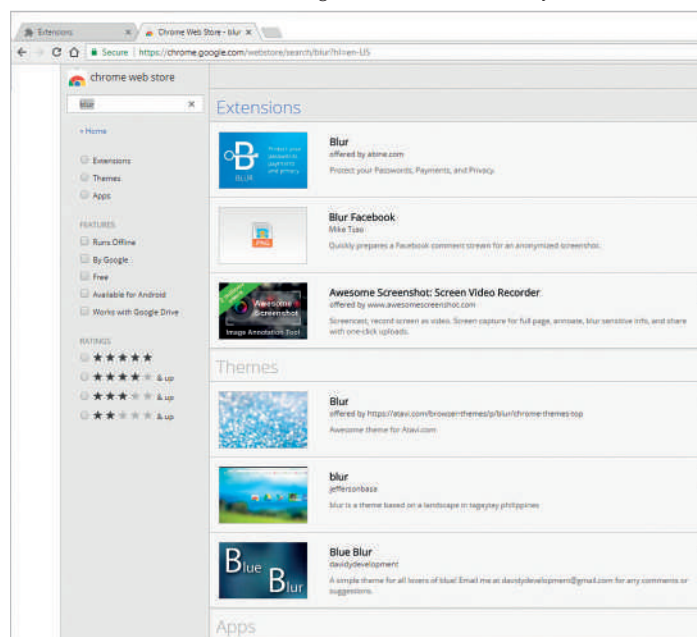
STEP 8 Under the Downloads section, it's an idea to tick the box Ask where to save each file before downloading. Again this can be a bit of a pain for the user; however it stops malicious background downloads from infecting your system, giving you more control and the ability to stop the process.



STEP 9 To the left of the Chrome Settings page you can see links for Extensions, Settings and About; click the Extensions link. With the Extensions page open, scroll down to the bottom and click the Get More Extensions link.



STEP 10 With the Chrome Web Store launched, via the Extensions link, search for Adblock Plus. Within the results, click on the Add to Chrome button on first option for Adblock Plus. This will install an advertising blocker within Chrome, securing you from any threats from Internet advertising. Do the same for Blur (an anti-tracking add-on) and HTTPS Everywhere.





How to Secure Your Home Network

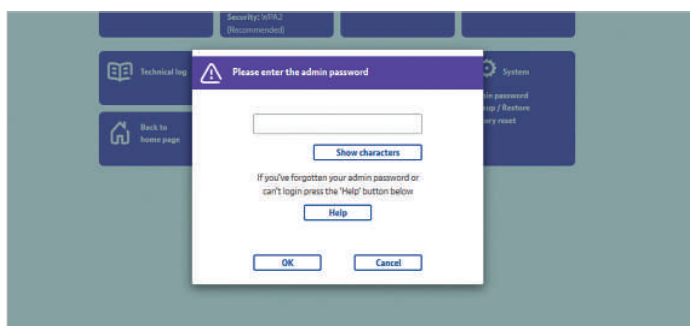
We've mentioned previously that an attack doesn't always come from the other side of the globe but can indeed be a little too close to home at times. Home network hacking is possible with the simplest of tools available on the Internet, often even just tapping into a cable.

Network Protection

Without being too paranoid, it's remarkably easy to get into a neighbour's home network. If you live in a block of flats or you use powerline adapters, you may need to consider these ten steps for better network protection.

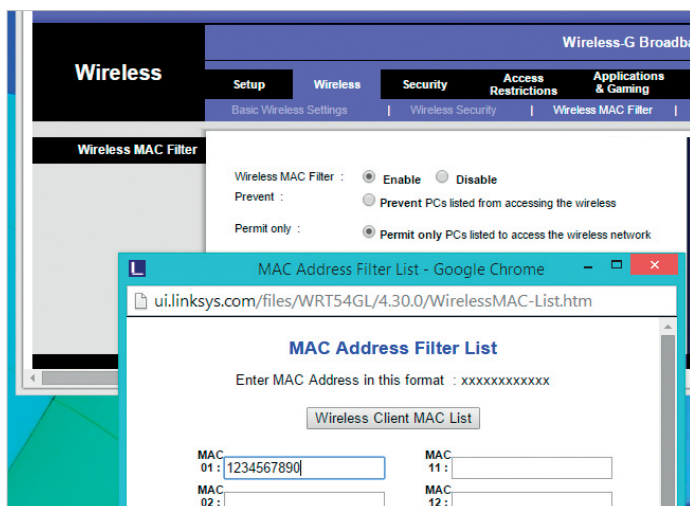
ROUTER PASSWORD

The most common entry point to gain access to your network is via the router. The router from your ISP may well be offering the latest forms of encryption but it doesn't take a genius to trawl the less reputable sections of the Internet to obtain a list of passwords. Therefore, change the default username and password to access it.



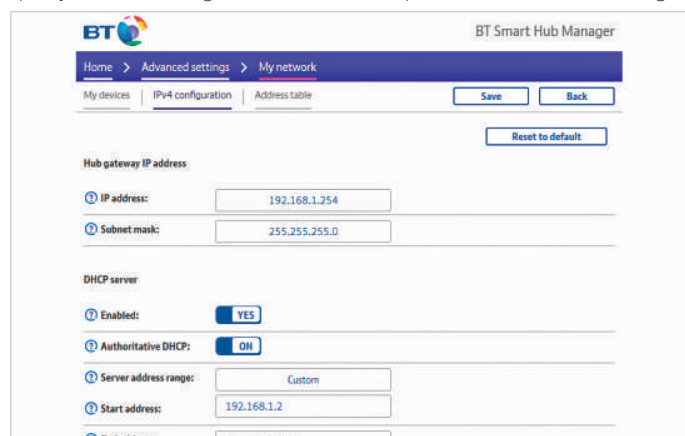
MAC ADDRESSING

Most routers these days come with a form of authentication called MAC (Media Access Code) address filtering. Every networkable device, computers, tablets, games consoles, come with a unique MAC address. The filtering allows you to enter the MAC addresses of your devices, so only they can be used on your router. Consult your router documentation for more details.



DISABLE DHCP

It can be a pain but try disabling DHCP on your router and opting for static IP addresses. Every device that connects to a DHCP router will receive an IP address. By eliminating that you get to specify the address range available. It's not fool proof but it's worth considering.



POWER OFF

According to Trustwave's 2013 Global Security Report, many home network hacks are conducted when the household is away or asleep. This leaves the hacker with ample opportunity to steal bandwidth and view files you may have on a NAS drive. The short, simple solution is to power off the router at night and if you go out for the day.





POWERLINE ENCRYPTION

Powerline adapters are an excellent resource for connecting wired network devices, without trailing lengths of cable around the home. However, depending on the adapter, it is possible to use another adapter to gain access to yours. Newer homes are common where you're able to pick up another network, so use the encryption button if the adapter has one.



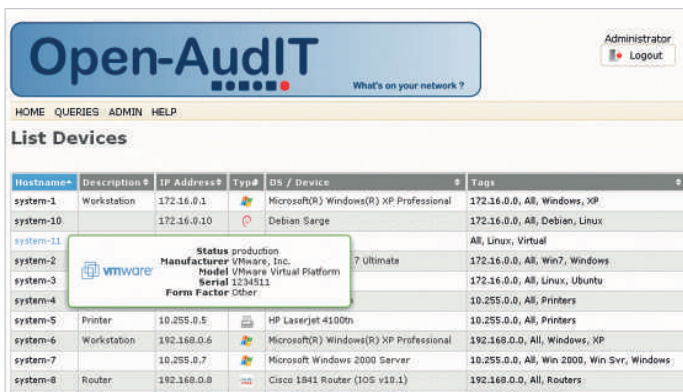
ETHERNET CABLES

Cabling a home with Ethernet isn't a difficult project, this offers faster connection speeds than that of wireless; but if you're living in shared accommodation or a flat block, make sure that any unseen cable lengths can't be accessed by a neighbour. It's easy enough to splice into an Ethernet cable and steal bandwidth.



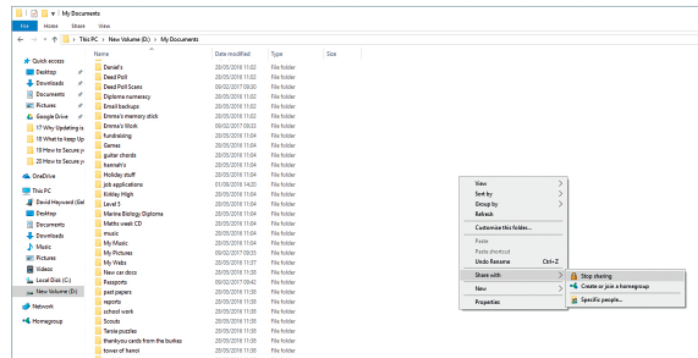
NETWORK MAPPING

Consider using a network mapping program, such as Open-Audit, to gain a better understanding of what devices are attached to your network. Become familiar with the addresses, manufacturer, model IDs and so on of every connected object. That way, should anything new appear, you'll know it's not something you allowed.



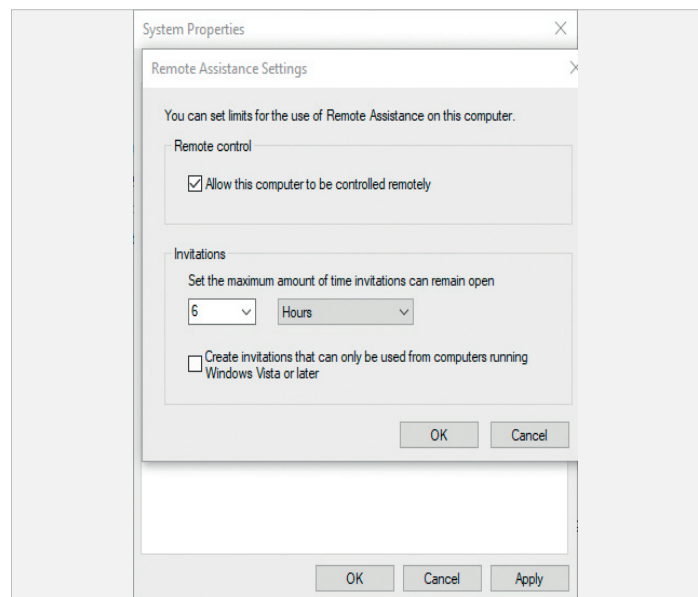
SHARE LESS

Sharing resources and files from one computer to another is perfectly fine but consider sharing less if you live in close proximity to others. Once a hacker has gained access to your network, getting to any shared folders you have will be a doddle. In extreme cases don't share anything but generally tighten password control.



REMOTE ACCESS

Remote administration on both the router and computer certainly help you out when you're not at the keyboard. Perhaps you connect to your home network from work? Whatever the reasons, it does leave a potential gap in your home network security. Consider closing it completely or double-checking the authentication is top notch.



VISIBLE PORTS

If you run a small office make sure that all your wall ports are located in areas where they are secure. Behind desks and generally away from where the public or any visitors may be able to sneakily plug a laptop in.





What are Wireless Security Standards?

Wireless security has adhered to a number of standards since 1999, each improving over the last due to the ability for a then-modern computer to hack the security levels behind them. Tighter controls are needed as computers and the way they connect have become increasingly more complex.

WEP, WPA, WPA2, IEEE...

Amid the confusing acronyms lies a logical progression of wireless encryption and security protocols. Whilst at first they seem bewildering, it's quite interesting to learn of their history.

The technology behind delivering a wireless network has evolved over the last couple of decades and so has the ways and means in which to secure it all. It's not just simply down to choosing a password that no one is likely to guess, you need to make sure that data and connection to a wireless network is encrypted to the highest possible standard.

These standards are always moving forward and like most elements of the technology industry they come with a bewildering cocktail of acronyms and meanings. Encryption and all things security can be a confusing topic, even for experts. Here are the current, and most important, terms you should be familiar with when talking about wireless security standards, wireless networking and the hardware that lies between your wireless communications.

IEEE

The Institute of Electrical and Electronics Engineers is the organisation responsible for setting the entire wireless security industry, and data communications standards. It was founded, surprisingly, back in 1963 and is regarded as the largest association of technical professionals in the world.



802.1x

You've no doubt come across the numbers 802.11 when looking at wireless-based and networking documentation but what on earth does it mean? 802.1x is the IEEE standard for providing authentication and controlling user traffic across wireless and wired Ethernet-based networks. It's an ideal application for providing authentication for wireless networks, as it requires very little processing power from the authenticator: the actual wireless access point. The better the standard, ending with a, b, g, n, ac and so on, the higher the speed of communications between devices.



WPA2

WPA2 is the upgraded standard security technology of WPA. It's designed to offer the user an impressive 256-bit encryption key, which is virtually uncrackable unless you're a secret research lab with a few billion dollars to spare on quantum computing and dedicated hardware decrypting processors. There are also different sub-standards within WPA2, with AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol), both of which are encryption methods, along with the lesser used CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).



WEP

This is the original wireless encryption security standard, Wired Equivalent Privacy. Whilst the protocol worked for the late nineties wireless networks, it was soon overshadowed by the ever increasing power of the average computer. WEP uses a 40-bit standard encryption key, which is a key consisting of either 10 or 26 hexadecimal digits. That sounds like a lot of possible keys to crack but a modern, powerful computer would be able to break 40-bit encryption in around 30 seconds; compare this to months for a computer in the late '90s.



Access Point

Talking about access points, this is the hardware that acts as a receiver or transmitter for the wireless signal and network. It can physically be a number of different components, such as a router, switch or powerline adapter but essentially it's the hardware that converts a wired Ethernet network to a 2.4GHz or 5GHz wireless signal and vice versa; it's also referred as the WAP, Wireless Access Point.

WPA

Replacing the WEP standard, WPA (Wi-Fi Protected Access) provided a much needed improvement for the ever advancing march of security. It became the standard in 2003 and offered the user either 64-bit or the more adept 128-bit key levels of encryption. A 64-bit key attack would take several lifetimes when it was first introduced; these days it's estimated that it would take several months, maybe less if the attacker used several computers working as a cluster. Naturally 128-bit key lengths are mind-numbingly more complex and even by today's standards, the theoretical process of a brute force attack would take more time than the universe has estimated left to exist. Which is a very, very long time.



How to Secure Your Wireless Network

It may seem a little far-fetched but it's not unfeasible for a hacker to sit outside your house with a tablet or laptop and gain access to your home network via the router's Wi-Fi signal. Understandably it's quite rare but it's worth considering beefing up your protection.

Wi-Fi, Lock and Key

A lot of the standard tips on protecting your Wi-Fi merge with those of protecting your wired network. It's common sense mostly and keeping an eye on what's going on in your own network.

ADMIN PASSWORD

All routers come with a generic username and password. Depending on the model and manufacturer of the router, it's surprisingly easy to get hold of the username and password. For example, view www.routerpasswords.com and choose your router. With that being the case, change the administrator username and its password.

RouterPasswords.com

Welcome to the internet's largest and most updated default router passwords database.

Select Router Manufacturer:

BELKIN

Find Password

Manufacturer	Model	Protocol	Username	Password
BELKIN	F5D8130	SNMP	(none)	MinAP
BELKIN	F5D7150 Rev. FB	MULTI	n/a	admin
BELKIN	F5D8233-4	HTTP	(blank)	(blank)
BELKIN	F5D7231	HTTP	admin	(blank)

If you can't find the exact model of the router you are looking for, try a password from an alternative model from the same manufacturer. Usually, vendors use the same or similar passwords across different models.

Copyright © 2016 RouterPasswords.com. All rights reserved.

CHANGE SSID

The Service Set Identifier (SSID) is the name of the router that's broadcast so you're able to locate and connect to it. Most routers will display the name and ISP, or the make and model, making it easier for a hacker to find the information they need to gain access. It's recommend therefore to frequently change the SSID.

BT Smart Hub Manager

Home > Wireless

Change settings Back

Here you can see your BT Smart Hub's wireless settings. If you want to change anything, click on Change settings to go to the advanced wireless page where you can customise your set-up.

2.4 GHz and 5 GHz

Wireless: On

Channels: 2.4GHz - Smart (Channel - 11)
5GHz - Smart (Channel - 36)

Network name: BTHub6

WPS: On

Band steering: Off

Security type: WPA2 (Recommended)

ISP PASSWORD

ISP supplied routers tend to have their own set of usernames and passwords. Although these are more secure than that of the default set, they are still obtainable from the more dubious quarter of the Internet. A potential hacker will easily be able to get hold of subsets of passwords, so where possible change the ISP default username and password.

Dynamic DNS 5 GHz channel: Smart (Channel 36) Address table

Security: WPA2 (Recommended)

Technical log Please enter the admin password

Back to home page

Show characters

If you've forgotten your admin password or can't login press the 'Help' button below

Help

OK Cancel

HIDE SSID

It's also possible to select an option to hide your SSID from being broadcast. Whilst this doesn't stop it being hacked, it does make it a little more difficult for someone who's casually looking around for networks to access. You'll need to consult your router documentation to find how to hide your SSID for make and model.

LINKSYS A Division of Cisco Systems, Inc.

Wireless

Setup Wireless Security Access Restrictions Applications & Gaming Administra

Basic Wireless Settings Wireless Security Wireless MAC Filter Advanced

Wireless Settings

Wireless Network Mode: Disabled

Wireless Network Name (SSID):

Wireless Channel: 1

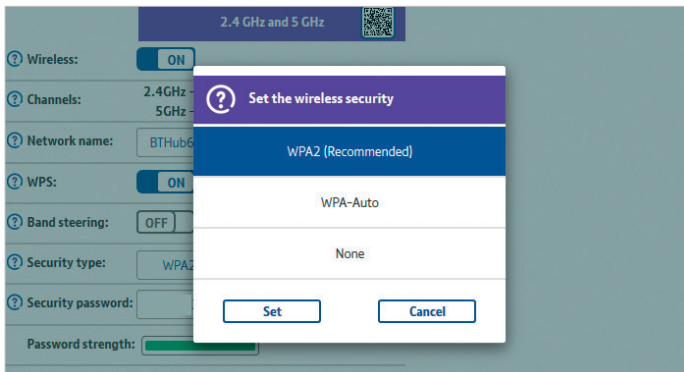
Wireless SSID Broadcast: ☐ Enable ☒ Disable

Save Settings Cancel Changes



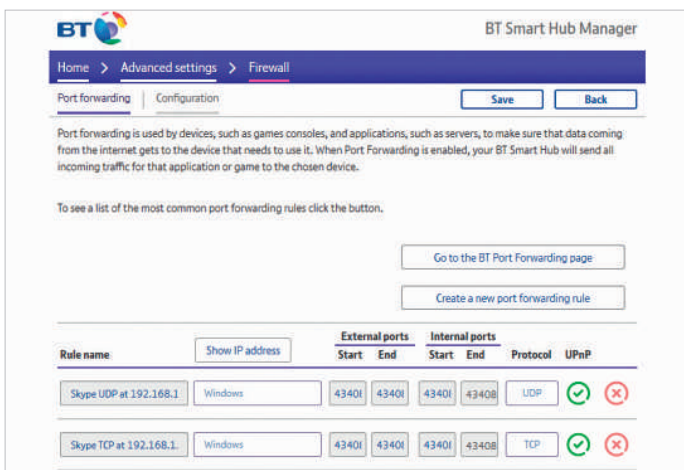
USE WPA2

Most modern routers will already come with the latest security standard enabled, WPA2; but there are instances of some routers defaulting to a lesser security type for the sake of device compatibility. It's essential that you ensure your router is using the latest and best form of encryption for your protection.



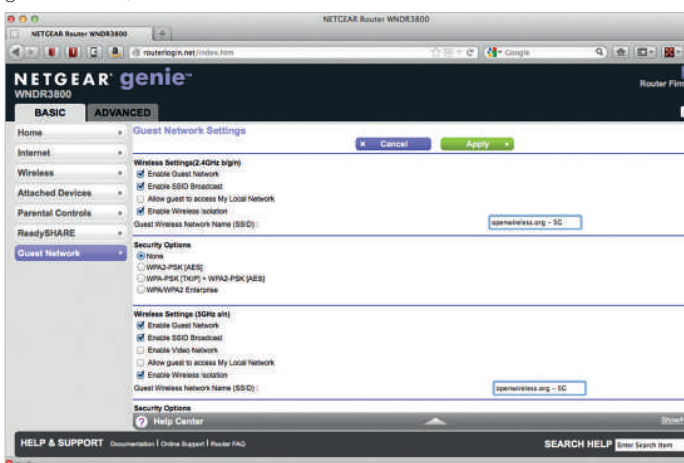
ROUTER FIREWALL

The firewall that comes with Windows is good but the firewall from third-party AV software is even better; and for extra protection, make sure that the router's firewall is enabled and doesn't have any potential leaks.



DISABLE GUEST

Some routers come equipped with the ability to allow a guest network. This enables users to connect to the router without requiring an encrypted password. Obviously this is a potential huge gap in your home network security. If you have no need of a guest network, then look to the documentation on how to disable it.



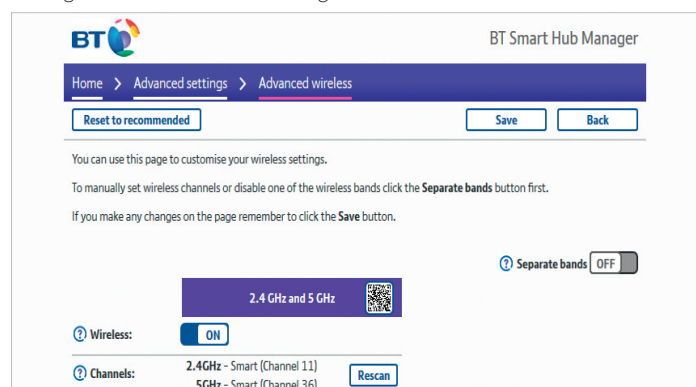
ROUTER RELOCATION

Most users will have their router located in the living room, near the master phone socket. This means that not only will the router broadcast through the house, it's also broadcasting over much of the street in front. Consider placing the router in a more central location of your house. This offers great coverage, whilst limiting its signal reach beyond.



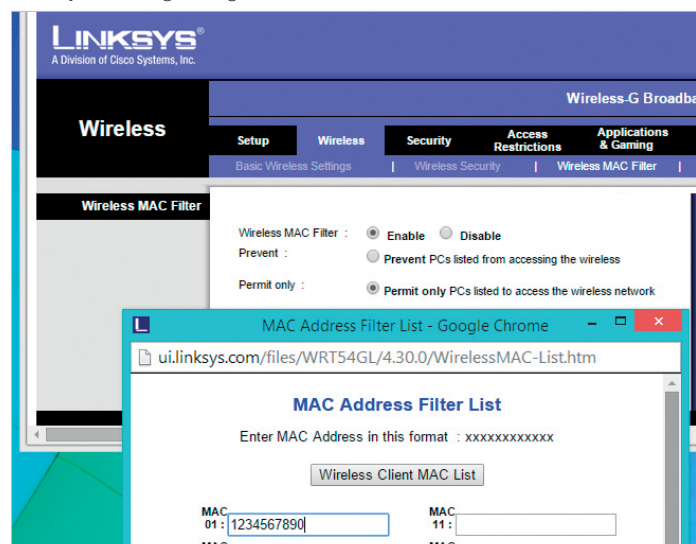
DISABLE WPS

The WPS button on a router and a device will allow easy pairing of the two without the need to enter the encryption password. This is certainly convenient but someone who may gain physical access to your router will be able to pair their own device. Look to turning off WPS in the router's settings.



MAC FILTERING

Filtering MAC addresses was discussed previously but it's worth repeating with regards to wireless network security. By filtering those devices that are allowed to connect to your router, and keeping an eye on what's connecting, you're able to control your security to a far higher degree than usual.





What is Encryption?

We've mentioned encryption and its impact on your privacy and security, but what exactly is it? The definition of encryption is 'the process of converting information or data into a code, to prevent unauthorised access'.

Kryptos Communications

To better understand encryption it's worth taking a moment to learn about its origins, how it's been developed over the years and how it applies to our modern communications.

The word encryption comes from the ancient Greek word Kryptos, which means hidden or secret. Interestingly, the use of hiding messages from others can be traced back to early Egyptian scribes who inserted non-standard hieroglyphs within other communications in order to hide the message from casual viewers. According to historians the Spartans used strips of leather with messages engraved. When the strips were read they were meaningless but when wrapped around a staff of a certain diameter the characters would be decipherable.

Of course, the modern forms of encryption are far more advanced but the overall core concept has remained the same: to be able to send a message to others without anyone else being able to decipher it. However, modern encryption now requires more than simply sending coded messages. Not only is confidentiality required, encryption must perform a level of authentication, so the origin of the communication can be verified; integrity of the communications, where both the sender and those who receive the communication can be ensured that the message hasn't been altered in between; and some form of nonrepudiation, where the sender cannot deny having sent the communication in the first place.

During the early digital age the only users of encryption were the government and military, and as such between them they created a set of algorithms and standards to protect the communication on the battlefield and from one government agency to the next. These algorithms grew in complexity as technology advanced and it wasn't long before the military-based forms of encryption were being used in commercial modes of communications. Within a few short years, bank transfers, cash withdrawals and data sent to and from modems began utilising these new protocols to protect sensitive information.

Today we're regularly seeing and using devices that boast 'military grade 256-bit AES' forms of encryption, a standard that is regarded as nearly impossible to break without spending billions on specialist hardware and software. In plain English, the modern form of encryption takes data and passes it through an algorithm together with a key. This creates a garbled file of characters that can only be clearly read if the correct key is applied to decrypt the data. Algorithms today are divided into two categories: symmetric and asymmetric.

Symmetric key ciphers use the same key to both encrypt and decrypt data. The most popular symmetric cipher is AES (Advanced Encryption Standard), developed by the military and government to protect communications and data. This is a fast form of decryption that requires the sender to exchange the key used to encrypt the data with the recipient before they're able to read it.

Asymmetric key ciphers are also known as public-key cryptography and utilise two mathematically linked keys, public and private. The public key can be shared

with everyone and is usually generated by software or provided by a designated authority. The private key is something that's usually only known by the individual user. Interestingly both types of keys can be applied, where one user has a public key and another a private key, which can be combined to form a shared encryption level.

These keys are many characters in length, proving it nigh impossible for someone to Brute Force hack them. The Brute Force method involves using a program on a computer to try every possible combination of a key until the correct one is found. In the case of the 256-bit encryption, it would take 2^{256} different combinations to break the key. If you were able to force one trillion keys per second, it would still take you somewhere in the region of 10^{57} years in order to crack 256-bit encryption. However, a powerful computer can probably manage around two billion calculations per second, so in theory it would take 9.2^{50} years for your standard desktop to crack it. Take in mind that the universe has theoretically only been in existence for 1.4^{10} years.

Numbers as big as that are generally far too mind-boggling to comprehend. Suffice to say that if you're able to use 256-bit encryption for your communications or to protect your data, then you're going to be protected for at least seven times the current age of the universe.

“

Encryption is the act of protecting your data from prying eyes

”



“Forms of encryption can be traced as far back as ancient Egypt, using non-standard hieroglyphs.”

“Making data impossible to read is just one step, you also need the key to decrypt that data.”



“The universe is 14 billion years old, but it would take seven times that time to crack 256-bit encryption.”

ENCRYPTION



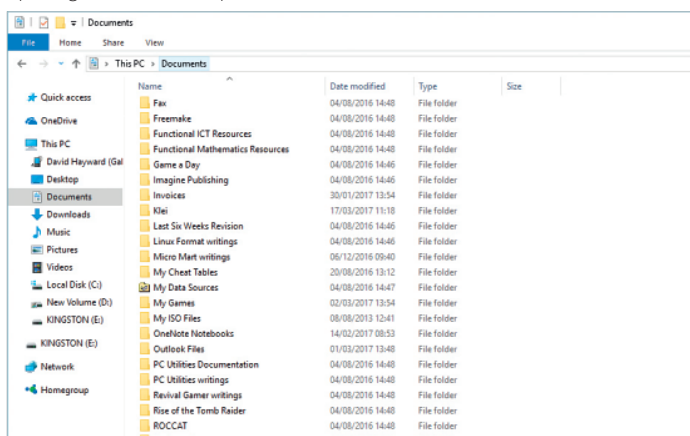
Encrypting Your Windows Laptop

Windows comes with Microsoft's BitLocker program to encrypt the file system; however, Windows Home versions do not have this feature. Thankfully there are many encryption programs available for download, we're using DiskCryptor in this tutorial.

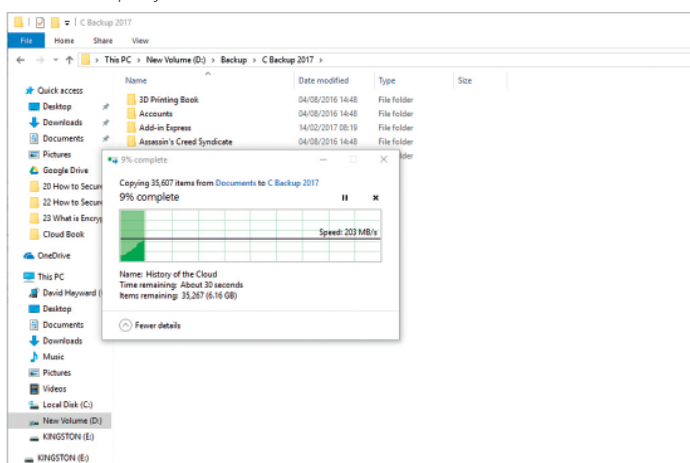
Windows, Under Lock and Key

We're going to encrypt a 2GB USB flash in this example, purely for ease of use and to demonstrate how you can encrypt your entire laptop hard drive(s).

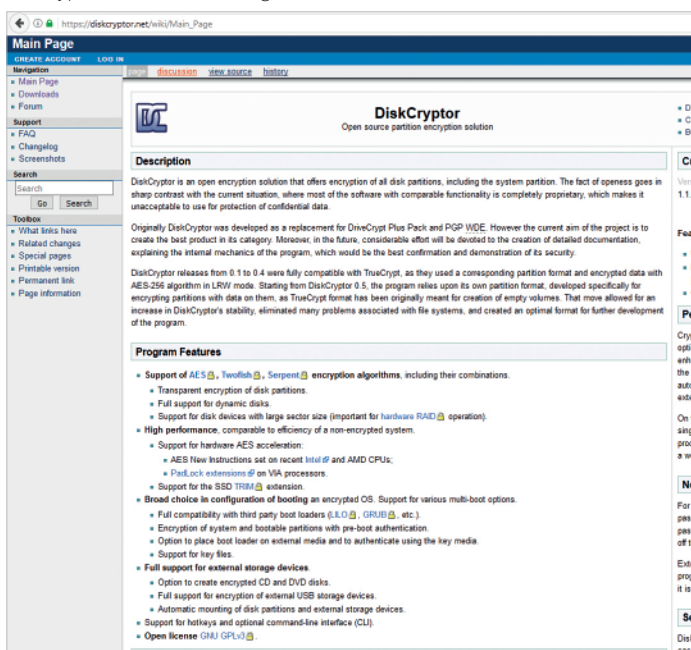
STEP 1 Encryption doesn't affect the core data, other than making it impossible to read without the decryption key but it's always worth making sure you have a backup of all your data prior to any system related changes. If you store your work or data in the Documents folder, then start by opening it in Windows Explorer.



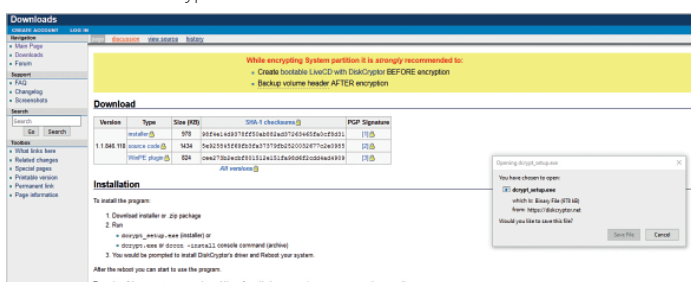
STEP 2 Press Ctrl+A to highlight all the files, then press Ctrl+C to copy them to the clipboard. Next, choose a suitable backup location such as an external or network drive and when ready, press Ctrl+V to paste the copied data into the new location. Then, should something go wrong, you have a recent backup of your most used data.



STEP 3 It's always best to ensure safe data before commencing with anything like this. It's also always worth doing (as we are) a test of the software first, on a disk that you don't mind messing up should you get the process wrong. Let's start by navigating to the DiskCryptor homepage, at www.diskcryptor.net/wiki/Main_Page.

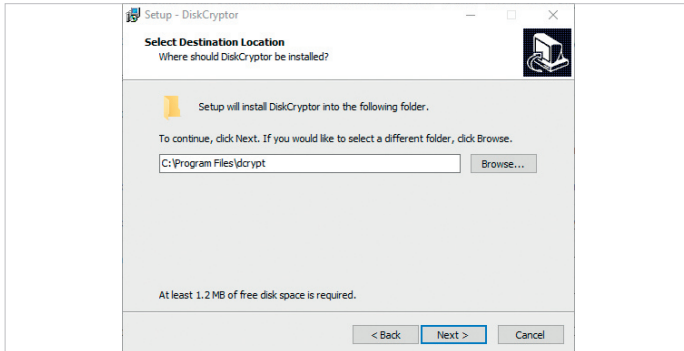


STEP 4 Using the menu to the top left, click on the Downloads link. Look for the latest version in the Download section and click the link for the Installer. This will open a confirmation box, click the Save File button to download the DiskCryptor executable file.

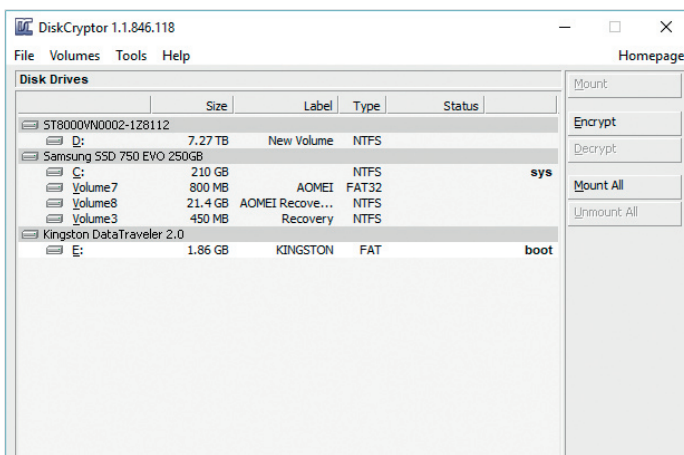




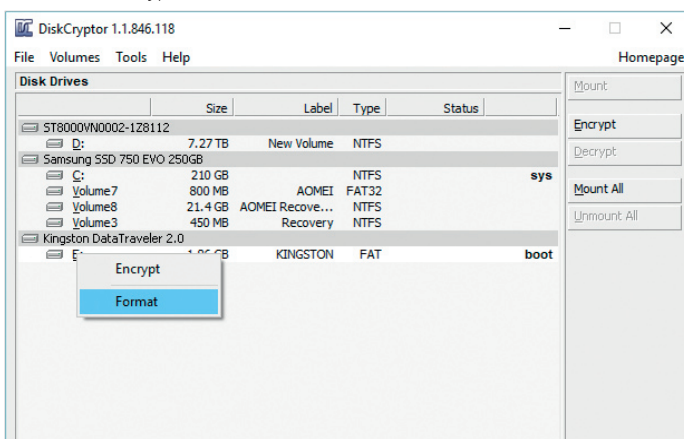
STEP 5 The dcrypt_setup.exe file should now be in your Downloads folder. Double-click it and select Yes to accept the Windows confirmation. With the DiskCryptor setup window open, click the Next button and accept the license agreement on the following page. For the remainder of the options choose the defaults, clicking Next. When done, click the Install button and reboot the computer.



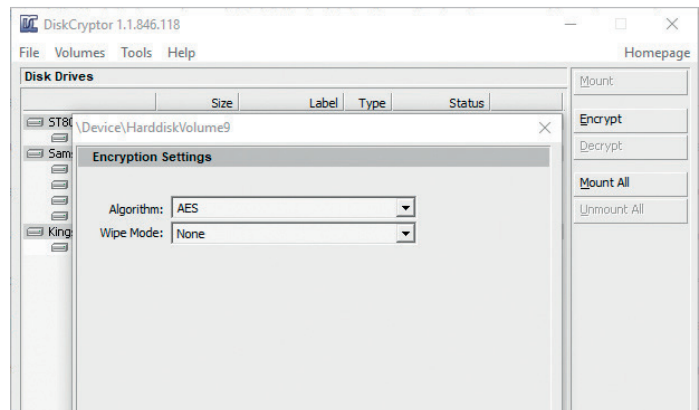
STEP 6 After a reboot, click the Windows Start button and locate the newly installed DiskCryptor program. You will need to click Yes to authorise its administrative access. With DiskCryptor open you can see the list of currently installed hard drives in your system. You can click each in turn and view its information at the bottom of the DiskCryptor window.



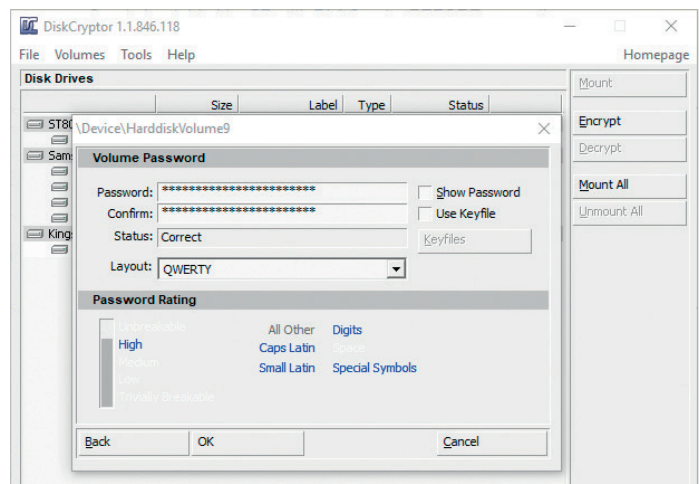
STEP 7 Start by selecting the disk you want to encrypt. In our example, as mentioned before, we're going to test this out on a USB stick. We recommend you do too, until you're comfortable with the process. With the correct drive selected, either click the Encrypt button to the right or right-click and choose Encrypt from the menu.



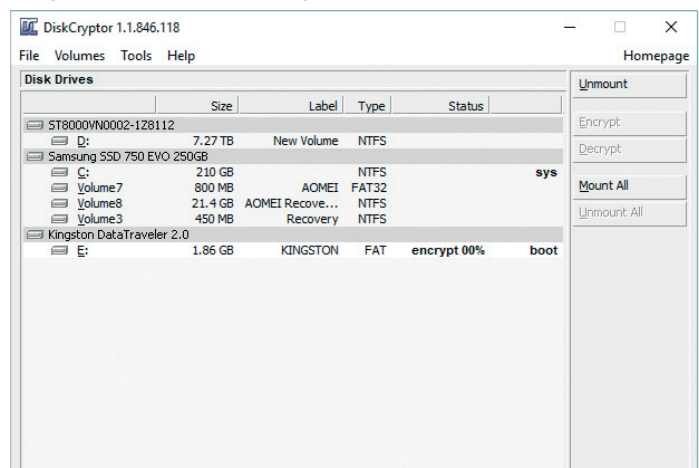
STEP 8 You're now offered a selection of available algorithms to choose from. Click the drop-down box to view them all but we recommend staying with the default AES algorithm for the time being. Leave the Wipe Mode box as None and when you're ready, click the Next button.



STEP 9 In the next section, choose a unique password for accessing the encrypted disk; you're notified how strong the password is. When you're ready, enter it again in the Confirm box. Click the OK box to start the encryption process.



STEP 10 Depending on the size of the drive, and how much data there is on it, the encryption process could take some time. When it's complete you're notified and the selected drive will be fully encrypted, with you being able to access and decrypt it using the password you set up in the previous step.





Top Ten Encryption Tools for Windows

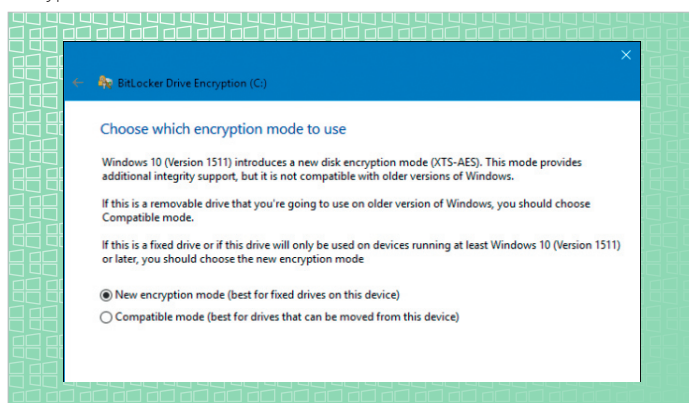
There's no shortage of programs that can encrypt files, folders and entire drives for Windows. Whilst some are very good indeed, others tend to fall by the wayside by not offering a good solution.

Encryption Galore

Here are ten different encryption tools for you to consider that work well with Windows, and some previous versions too. Some are free, others cost but they're all good in their own right.

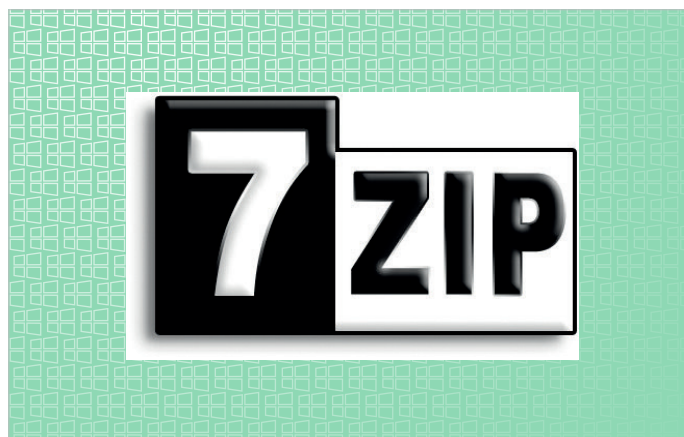
BITLOCKER

Available only for users of Windows Pro, Windows 8.1 Pro and Enterprise and Windows 7 Enterprise and Ultimate versions. If you're running the Home versions, you'll need to upgrade via the Microsoft site, or from the Windows Store. In short, BitLocker offers full disk encryption with 128-bit or 256-bit AES standards.



7-ZIP

Primarily a compression program, 7-Zip can also encrypt your data with the AES 256-bit standard. It's simple to use, completely free and comes in either 32-bit or 64-bit versions depending on which type your core Windows system is.



VERACRYPT

This is a free disk encryption program that's based on the popular TrueCrypt. It offers enhanced security, lots of levels of encryption and support for UEFI drives. It's available for Windows version 7 onwards as well as Mac OS X, Linux and even the Raspberry Pi.



AXCRYPT

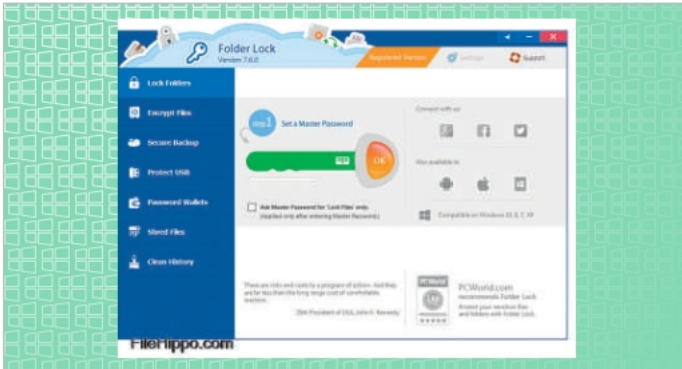
Another excellent free program, AxCrypt offers 256-bit encryption, easy to use interface, cloud storage integration, password management, secured folders and is available in a multitude of different languages. There's support for Windows Vista onward as well as support for files sizes over 4GB.





FOLDER LOCK

An excellent and comprehensive folder locking program, with support for 256-bit encryption and Windows versions from Vista onward. It costs in the region of £40 but you'll need to check for the most recent pricing. For your money, you get secure backups, USB protection, password wallets, a secure file shredder and much more.



GPG4WIN

This entry is a little more advanced but once you master its intricacies it's an extraordinarily powerful program, and free. It's designed for file and email encryption, offering incredible levels of security for Windows 7 upwards and Microsoft Outlook 2003 and newer.



CRYPTOEXPERT 8

Costing around £60, CryptoExpert 8 offer support for Windows versions from 7 onward, unlimited file size encryption, 256-bit AES encryption, unlimited secure file vaults and on the fly encryption as you move and copy files around your system.



DEKART PRIVATE DISK

This is a simple and easy to use program that supports AES 256-bit encryption, compatibility with Windows Mobile, free unlimited support and updates; and it also includes its own firewall to help prevent hackers from gaining access to your system.



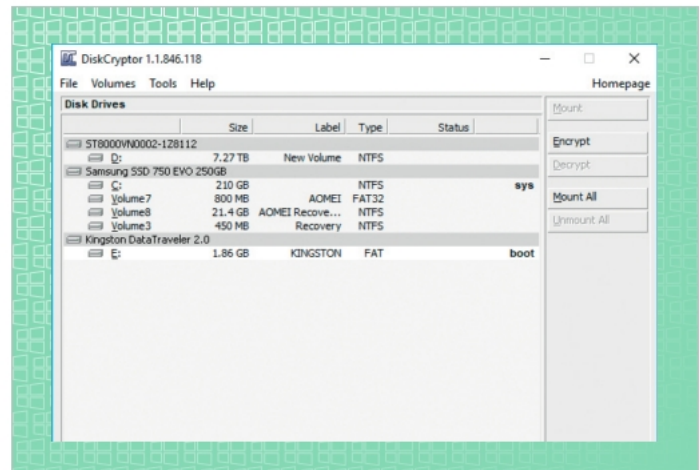
CERTAINSAFE

This is an interesting product, as it provides cloud-based encryption for any files or folders you upload into your online storage. It offers AES 256-bit encryption and an easy to use setup and integration into your cloud provider. It's Pay as you Go, so you only pay for what you use.



DISKCRYPTOR

We used DiskCryptor in the previous tutorial as it's a fairly straightforward program that can achieve high levels of encryption with ease. There's a lot more you can do with it and you can get further support from within the product's homepage.





What is a VPN?

Your system may be secure to any online threats but it doesn't always mean your privacy is assured. This is where a VPN comes in, as it offers the user a heightened level of anonymity when online and even another level of security and protection.

Virtual Private Network

Using a VPN can help hide your online presence. Whilst this may seem like an ideal way to get to illegal content, it's actually designed to help fight for your basic right to Internet and digital privacy.

Essentially, a VPN (Virtual Private Network) is a server or group of servers in a remote location that you can connect to through a client. The VPN servers then hide your Internet-bound IP address with their own, so if you connected to a VPN that's located in Australia then your IP address would be as if you were actually sat at a desktop down under.

The benefits of this are many but mainly a VPN will allow you to access region restricted websites, protect you from tracking and shield your browsing activities from those who want to find out where you are personally based. Obviously there comes a negative side, in the form of being able to access content that your country has deemed illegal for some reason but on the positive, VPNs have allowed people in countries with extraordinarily tight restrictions to get access to the outside world; often enabling them to report on what's going on in their own country to the world.

However, for most users having a VPN means they're able to gain access to TV channels in the U.S., Canada, Europe and other parts of the world. It's not always about being able to moderately 'cheat the system' by forcing the Internet to think you're somewhere else other than where you actually are though. Remote workers and employees who live in other countries can connect to company VPNs and be able to use the company's network resources as if they were physically sat in the building.

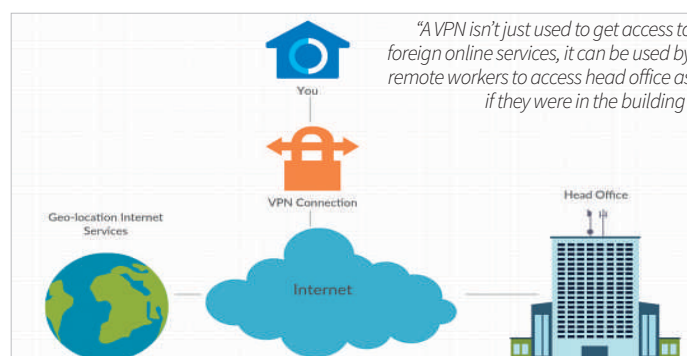
The connection from your computer to the VPN server, via the client, is usually secure to the tune of 256-bit encryption levels, depending on the VPN company who is hosting the service. All your Internet traffic will filter through the VPN server's systems, offering multiple layers of protection from viruses, malware and privacy. Beyond the other possible scenarios, using a VPN whilst you're abroad, working in a hotel for example, will enable you to access your home country's services and work resources. One more element that's worth mentioning is that using Wi-Fi hotspots is one of the biggest security risk for travellers; using a VPN can effectively improve your security whilst using a café's free Wi-Fi.

Most operating systems come with the ability to connect to a VPN through their network settings. If you have the network and connection details of the VPN in question, then you're able to connect to it using the built-in Windows, Linux or macOS options. However, the more common, and in some respects, easier method, is to use the client which most VPNs now offer as standard. The client is often simply a connection window that will ask you your login details, then provide a method of allowing you to connect to any of provider's geo-location servers, listed by country. Once the choice is made, you simply click the connect box and within a few seconds your IP address will be located within the chosen country.

There are plenty of VPN providers to choose from and we'll look at ten of the most popular in a while. Some offer a free connection service that's handy for quick browsing but isn't very fast. To gain access to faster servers, with better security and protection features you need to pay a monthly or annual subscription fee.

Thankfully it's not a lot, for the most part: you'll be expected to pay in the region of £5 to £15 per month. This grants you better coverage and the ability to use up to five or more different devices, including tablets and phones.

Over the coming pages we dig a little deeper into VPNs, as you can imagine, using one will significantly improve your protection when online. In terms of Windows security, the use of a VPN is quickly becoming vital, so by the end of this chapter you'll be knowledgeable and helpfully utilising one to your own advantage.



“

Using a VPN will protect your access online and filter all your Internet traffic through its secure service.

”



“You’re able to access web pages and Internet services from all over the world, even if you can’t from your own country.”



“A VPN greatly improves security for devices and when you’re using free Wi-Fi at cafés and other such locations.”





How Can a VPN Improve Online Security?

We've emphasised the enhanced privacy that a VPN offers when you're connected to its services, and the heightened levels of anonymity, but what security benefits does a VPN bring to a Windows computer with an antivirus program already installed?

Security Beyond Anonymity

It's a good question: how can a VPN improve Windows security? Whilst the privacy side is well catered for, there are some good security enhancements and features a VPN brings to the table.

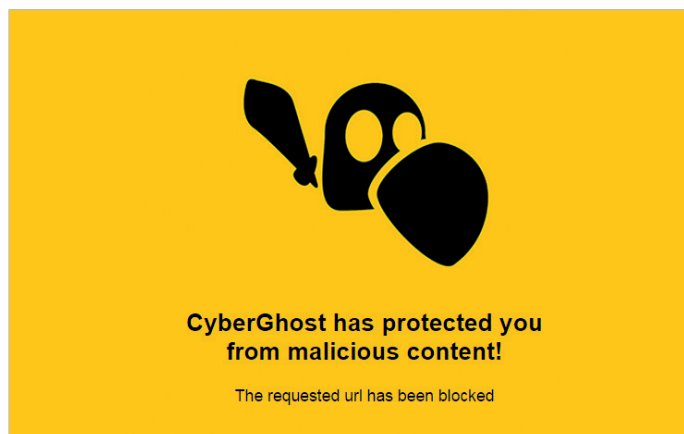
BROWSING ACTIVITY

This doesn't happen often but an ISP can become compromised and details of user activities leaked or stolen. Using a VPN can hide your browsing activity from trackers and even your ISP, enabling you to browse with freedom of fear of having your details leaked or accessed by others.



THREAT PROTECTION

To expand the previous feature, VPNs will filter web pages that are dangerous or contain threats. Even with a good antivirus client installed, you can still access a dangerous site. Using a VPN will stop the site from even being loaded.



ANTIMALWARE

Many VPN providers utilise a level of antimalware into their security layers. This enhances your security by filtering any downloads through the VPN first. Should there be a virus present, then it can be removed or stopped at the VPN before it even reaches you.



HIGHEST ENCRYPTION

The connection between you and the VPN server is encrypted to the highest possible standards. This makes it near impossible for some external element to gain access to the data you're transmitting. Online banking and shopping are extremely secure with a VPN.





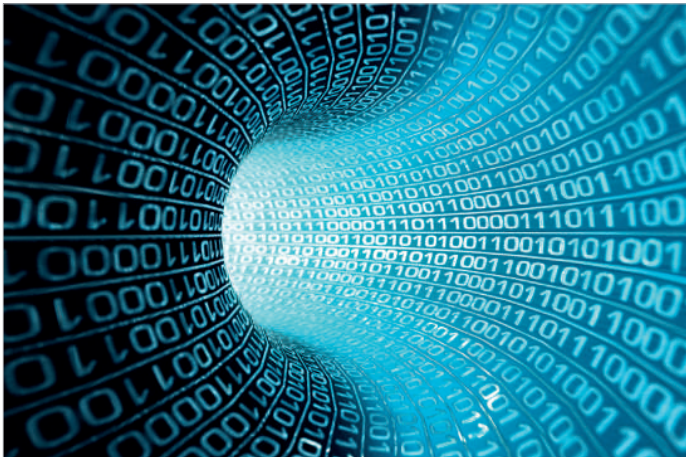
WI-FI PROTECTION

Public and free Wi-Fi hotspots are notorious when it comes to mobile security. Anyone with a little knowledge and some free tools via the Internet can intercept public Wi-Fi network and hijack your connection, revealing all your data. A VPN will encrypt the data and protect you.



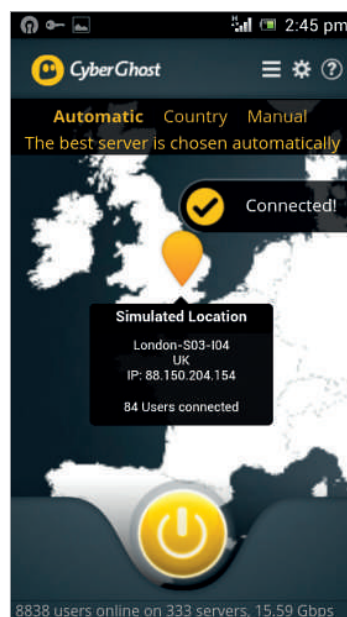
SECURE TUNNEL

If you're working abroad, or you're a remote worker, then a VPN connection to the company's servers will ensure that all the sensitive business data will remain secure. It's difficult for a company to ensure 100 per cent security with mobile and off-site workers but a VPN will provide a secure tunnel straight to the company itself.



MULTI-PLATFORM

The availability of iOS and Android VPN clients means that your call data and data stored on your device is also secure. Mobile VPN apps will use the same levels of protection and security, so your data can't be stolen when you're not even aware of it.



AD BLOCKING

Most VPNs will also add an extra layer of security whereby they actively block any advertising from websites. Internet ads are a necessary evil in some ways, as they provide much needed funds for your favourite freely available websites. However, some contain malicious content and need to be blocked.



USE HTTPS

Using HTTPS instead of HTTP uses the secure side of the Internet protocol. Sadly, it's not always implemented in browsers or by users. Many VPNs will force all websites to use the secure connection that a HTTPS site offers, enhancing your browsing security.



ZERO LOGS

In some countries data retention laws are quite archaic, with governments and other bodies being able to access your data log for as long as you've been able to access the Internet. A good VPN won't detail any logs of your browsing and in most cases won't even hand over any personal information relating to you to other agencies.





Top Ten VPNs

There's no shortage of programs that can encrypt files, folders and entire drives for Windows. Whilst some are very good indeed, others tend to fall by the wayside by not offering as good a solution.

Encryption Galore

Here are ten different encryption tools for you to consider that work well with Windows, and some previous versions too. Some are free, others cost but they're all good in their own right.

CYBERGHOST

CyberGhost is our favourite VPN. It offers 256-bit AES military grade encryption, no logging, access to 27 countries and hundreds of servers, protected browsing, ad blocking, access to fast servers, unlimited traffic and bandwidth and an anti-fingerprint system. All for around £5.83 per month for up to five devices.



NORDVPN

NordVPN offers two levels of encryption, access to fast servers, no logging, a kill switch in case the VPN connection drops and you're still surfing and support for multiple devices and operating systems. It's well priced and is highly regarded among the press and media. Not bad for a mere \$5.75 per month (around £4.50).



HMA

Despite its colourful name, Hide My Ass VPN is considered to be one of the best services available. Along with the usual secure 256-bit encryption connection you get blistering speeds, access to over 300 locations, anonymous email use, a free web proxy access and free extensions for your browser. Expect to pay around £5 per month.



PUREVPN

With support for multiple devices, 256-bit AES encryption and access to 180 locations worldwide with 750 plus servers, PureVPN is a great choice for the home user. The cost varies depending on the package but expect to pay in the region of \$5.90 (around £4.58). Just as with all these VPNs, it's worth checking for the latest pricing.



**VPN UNLIMITED**

VPN Unlimited offers a full firewall service with anti-malware, ad blocking and anti-tracking. There's 256-bit AES encryption, over a thousand servers in 70-plus locations, support for up to five devices, fast servers and app support for iOS, Android and Windows Phone. Pricing varies but expect to pay around \$8.99 (approx. £6.97) per month.

**PRIVATE INTERNET ACCESS**

Private Internet Access VPN offers a wealth of features with its impressive service. 256-bit levels of encryption, no traffic logging, ad blocking, support for five devices and access to over three thousand servers across twenty five countries. It's surprisingly cheap too, at just \$6.95 (about £5.40) per month depending on the package you opt for.

**IPVANISH**

IPVanish is another highly regarded and awarded VPN service. For \$6.49 (around £5) per month depending on the package, you get access to fast servers, unlimited bandwidth, no logging, 256-bit AES encryption and support for up to five different devices.

**VYPRVPN**

VyprVPN is an exceptionally good service that offer access to fast servers, multiple device support, unlimited bandwidth and connection, 256-bit AES encryption and access to over seventy global locations and hundreds of servers. The Premium package costs just £5.83 per month for a one year subscription, but check regularly for any changes.

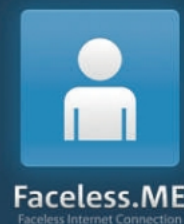
**TUNNELBEAR VPN**

TunnelBear VPN offers an initial 500MB per month free service, moving up to \$9.99 (around £7.75) per month for unlimited bandwidth. For this you get access to fast servers across twenty plus countries, 256-bit AES encryption and support for Windows, iOS, Android, macOS and browser add-ons.

TunnelBear

**FACELESS.ME**

Faceless Me is an interestingly named VPN service. Amongst its features expect to see elevated levels of encryption, unrestricted access, an easy to use interface and unlimited traffic. You get 2GB per month for free but for \$6.65 (around £5.16) you can have unlimited access and traffic.



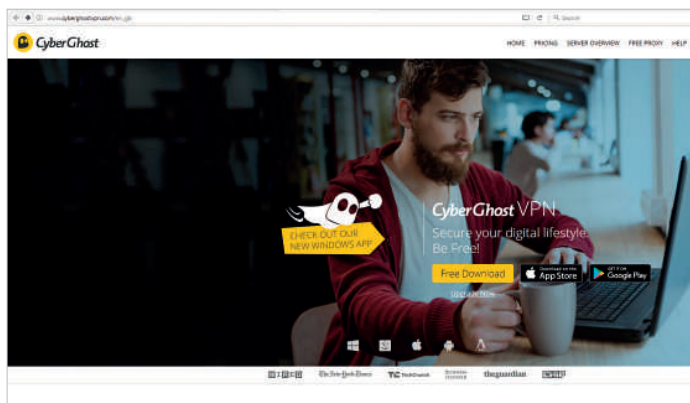
Using a VPN for Added Security and Privacy

We've covered how a VPN works, how it can improve your security and given you a top ten chart of recommended providers but we've not looked at how you would set one up and what it's like when up and running.

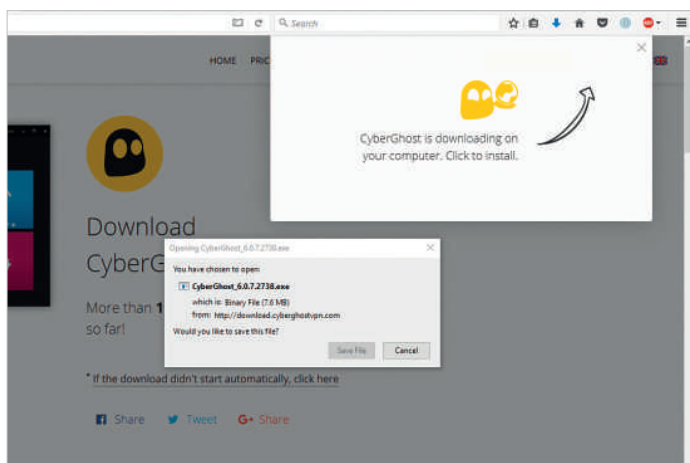
CyberGhost

We're going to use CyberGhost as the example VPN for this tutorial. You'll need to purchase one of the available packages to begin with, Premium is £3.74 per month, while Premium Plus is £5.83.

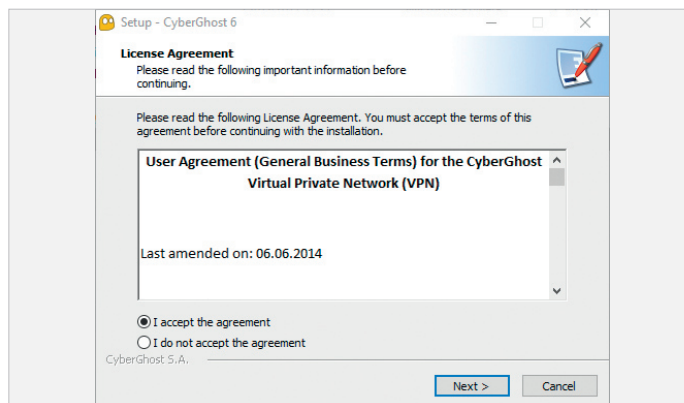
STEP 1 We won't use the free option in this instance, as the paid for services offer a better set of features with which to display the VPN in action. Start by navigating to www.cyberghostvpn.com and clicking on the Pricing link in the upper portion of the main CyberGhost site for your regional and latest pricing.



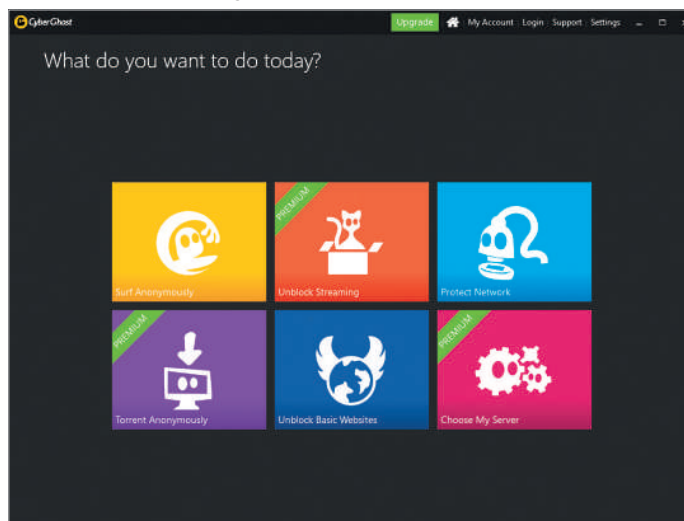
STEP 2 Assuming you've purchased one of the options, click the yellow Free Download button located in the top right of the main page. This will, after a few seconds, automatically initialise the download of the latest CyberGhost client software. Click Save File to download it to your Downloads folder.



STEP 3 Go to the Downloads folder and double click the CyberGhost executable followed by a click on Yes for the Windows authentication process. Accept the agreement and follow the on-screen instructions to set up CyberGhost on your PC; the default options are fine to use, unless you specifically require a different location for installation.

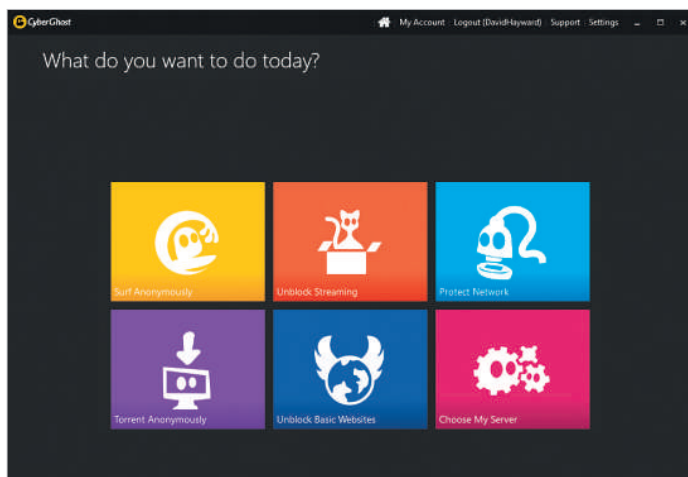


STEP 4 Once the installation is complete you're presented with the main CyberGhost client window. However, before you make a connection, click on the Login link located at the top of the client window.

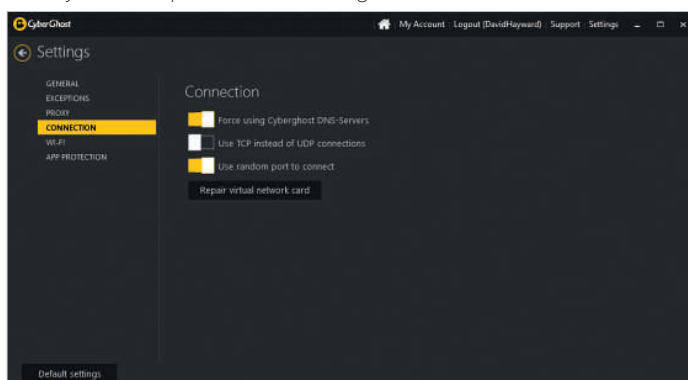




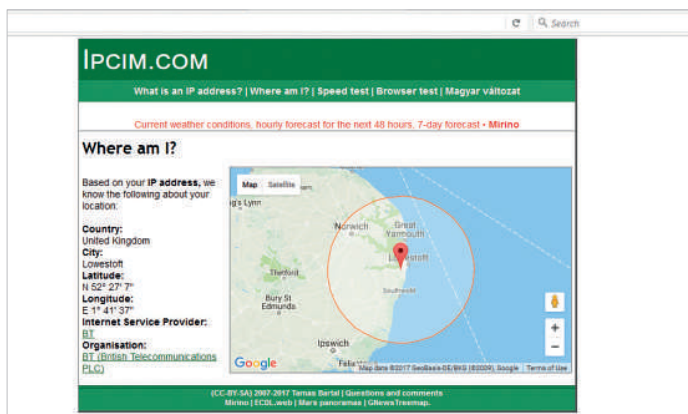
STEP 5 Enter your CyberGhost login and password that you set up when you purchased the package and click the OK button. Once the login is confirmed you're taken back to the main client window where the available options for the account package you purchased will be displayed.



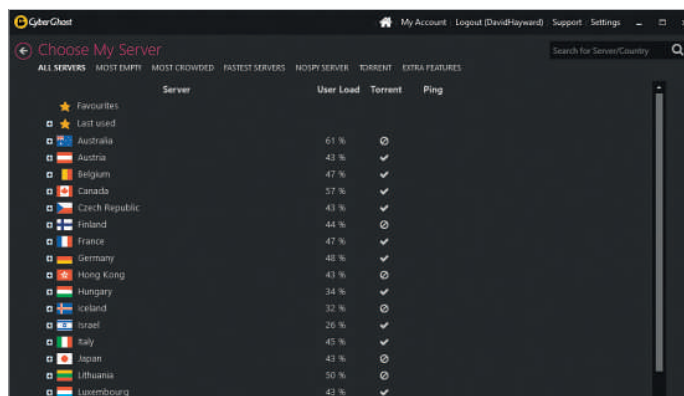
STEP 6 Before you use the service, it's best to check a couple of things. First click on the Settings link along the top of the client window. In here you can see multiple options for the control, connection and how CyberGhost will work with your PC. Generally speaking, the defaults are fine unless you have a specific reason to change them.



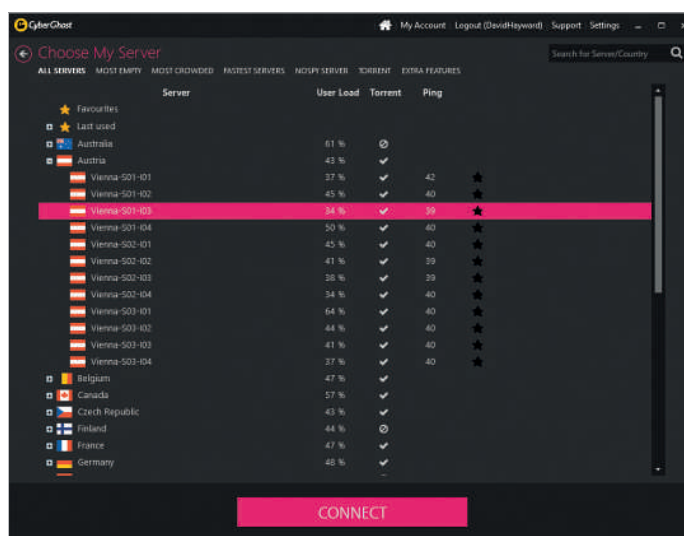
STEP 7 One more thing before connecting to the CyberGhost VPN: open a browser and enter www.ipcim.com/en/?p=where. This will display detailed information based on your IP address, such as the ISP you're using, the country, city, even latitude and longitude, complete with a map and possible radius you fall into. This is the kind of information we want to secure from prying eyes.



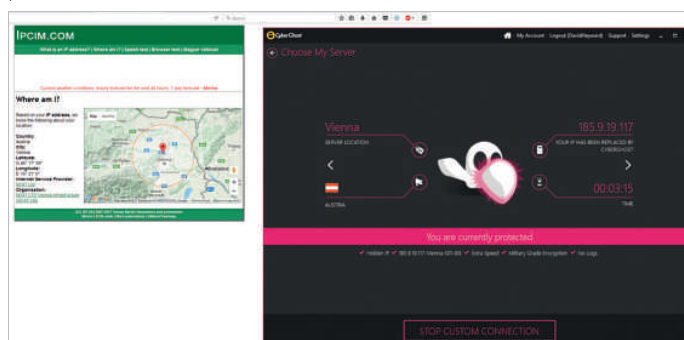
STEP 8 Click back to the CyberGhost client and return to the main window. Click the Home icon along the top of the client window and then the Choose My Server button in the bottom right. This allows you to choose your own server from the available countries that CyberGhost works with.



STEP 9 Look through the list and pick a server; we're going to use one of the Vienna servers in this instance. The Ping value is how fast the server is, the lower the ping the faster the connection. Either click to highlight the server followed by clicking the Connect button or double-click to launch the server connection.



STEP 10 The CyberGhost client will take a few seconds to connect. When it's ready you'll see a 'You are currently protected' message in the client. Close your browser and relaunch it, then return to the www.ipcim.com/en/?p=where page. You can see that the Internet now thinks you're located where the chosen CyberGhost server is, protecting and securing your privacy and personal details.







Online Protection and Recovery

While you can successfully protect yourself and your own computer, as soon as you make a connection to the outside world you're under the influence of many external factors. We look at how data is transmitted from your computer to the Internet and how a canny hacker can intercept that data for their own means.

Over the coming pages you'll discover how best to protect yourself and what strategies you can use to become more secure when online; even when you're out and about with your Windows laptop and other devices.

64	How Does Information Move Around the Internet?
66	How Can Internet Data be Intercepted?
68	10 Tips to Protect Yourself Against Interception
70	How to Secure Your Devices
72	How to Secure Yourself on Facebook
74	How to Secure Yourself on Twitter

76	Secure Yourself on WhatsApp
78	What to Avoid when Creating a Password
80	Password Generators and Tools
82	Top Ten Password Managers
84	Shopping Online and Security
86	How to Remove a Virus or Malware from a PC



How Does Information Move Around the Internet?

Before we get into online protection and disaster recovery, it's worth taking a moment to look at how information moves around the Internet, in particular your information. Just how is data sent from your PC across the Internet, to potentially fall into the hands of someone else?

Information Superhighway

The Internet is a huge, complex network of computers and is widely credited as humanity's greatest achievement. It's estimated that the Internet houses something in the region of 10^{24} bytes of information, which is quite a lot.

That estimated 10^{24} bytes equates to an exabyte of potential information held by every single connected device that makes up the Internet, some of which is your information. It's an impossible number to visualise, since we're only using gigabytes or terabytes of storage in most of our devices. More to the point though, how on earth does all that connect together, and how does it work?

To be able to transmit all that information, the data that travels around the Internet is in packets. Each of these packets contains a header and a footer. The information stored in the header and footer contains the details regarding the data being sent. For example, if you send an email to someone, as soon as you click the send button the data will be wrapped up in headers and footers, split into numerous packets and sent on its merry way.

Whilst that sounds logical, much in the same way a telephone call takes place, the reality is quite different. Those packets can take any route possible to get to the destination, as defined by the header and footer. Those routes don't necessarily all have to be the same either. Some packets may travel from one server to the next via one data pathway, while others will take another. The server at the other end will use the information provided by the headers and footers to collate the message, reform the data and present it to the email recipient the way in which you intended it to.

Remarkably, if the server at the other end detects missing packets it can request the missing information from its available connections. Any missing data can then be sent via an alternative route, updating the information as it goes so other packets will know that the previous route isn't getting through. The headers and footers then tell the server that the data packets are all present and what they should look like; the email will arrive accordingly.

All this happens in milliseconds. This sounds incredibly complex and on paper it makes the Internet appear to be a slow, lumbering beast dealing with incomplete packets of data. In a way that's how it works but instead of being a lumbering beast, the Internet or more accurately, the servers and computers attached to it, are fathoming data packets by the millions every second.

Just as we've seen, each computer on the Internet is connected using an IP address. These are registered across the Internet, so the headers and footers in each packet contain the IP address of the sender and where the data is heading to. That way, it's not just a random collection of data travelling across the ether in the hope of landing in the right place. The DNS, Domain Name System, converts the IP addresses to readable names, such as Google.com and the like, and back again. That way when you enter the email address someone@somewhere.com the DNS servers will convert the information and the packets sent to the relevant destination.

The protocols used throughout the Internet define what the data being communicated actually is. For example IMAP, Internet Message Access Protocol, is a mail protocol for accessing email on a remote server, such as accessing Gmail. These protocols help further the transmission of data to its intended location, making it more accurate and telling the computer on the other end what it is and how to piece together the jigsaw puzzle of packets that will be received.

Essentially this is how information is sent and received around the Internet. Obviously, there's a lot more going on in the background than we've mentioned here. The complexity that you can go into when dealing with data transfers is quite staggering and a little bewildering at times. Suffice to say, all those packets of data contain information about something or someone and somewhere out there are packets of data that contain information about you, where you are, what you're doing, and other personal details such as bank accounts, passwords, names and addresses.

“

The Internet is regarded as the greatest human achievement, and it's not difficult to see why

”



“Data is split into packets, with headers and footers telling servers what to do with it and where its going.”

“Along with protocols, packet information can take any possible route to its destination and it happens in a matter of milliseconds.”

```

Tracing route to www.bdmpublications.com [2a03:b0c0:1:a1:18a:f001]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  broadband.bt.com [2a00:23c4:7591:7200:ae84:c9ff:febb:f097]
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.
  4  16 ms  8 ms   8 ms   2a00:2382::1100:100:36
  5  10 ms  9 ms   9 ms   2a00:2380:300c:b000::e
  6  8 ms   8 ms   8 ms   2a00:2000:2000::4a
  7  9 ms   9 ms   9 ms   ae-6.r04.london05.uk.bb.gin.ntt.net [2001:728:0:5000::6b5]
  8  8 ms   8 ms   8 ms   ae-0.r24.london12.uk.bb.gin.ntt.net [2001:728:0:2000::5d]
  9  9 ms   9 ms   9 ms   ae-1.r25.london12.uk.bb.gin.ntt.net [2001:728:0:2000::152]
 10  11 ms  12 ms  11 ms   ae-2.r02.london01.uk.bb.gin.ntt.net [2001:418:0:2000::104]
 11  10 ms  11 ms  10 ms   2001:728:0:5000::af6
 12  *      *      *      Request timed out.
 13  11 ms  10 ms  10 ms   2a03:b0c0:1:a1:18a:f001
Trace complete.

```

“DNS servers translate IP addresses to readable locations, the packets then know where exactly to head to deliver the data.”





How Can Internet Data be Intercepted?

We've seen how data travels around the Internet in packets and with the help of various protocols that determine its source, destination and what manner of data packet it is. While that's all well and good, it's worth knowing how a hacker goes about intercepting that information.

The data packets that make up a message, or a string containing a username and password, are sent to and from yours and other computers without most of us ever really knowing what's going on in the background. It's this lack of knowledge that's the hacker's greatest tool. Well, that and some clever software that's freely downloadable from the Internet. Let's look at how data can be intercepted by a hacker. Let's use the scenario that you're on a business trip, or just out and about, and you're using a café's free, public Wi-Fi.

There are numerous, and quite ingenious, ways in which data can be intercepted by a hacker.

“

Man in the Middle

”

Normally you need to be using an unsecure network, such as a public Wi-Fi but there are other ways and means.

MITM

The first and most notable form of attack is called MITM or Man In The Middle. This attack utilises a set of free tools that can essentially grab data packets from the locally used network. This means that the data packets leaving your computer must travel through the free Wi-Fi's network before going off into the Internet to its destination. The MITM attacker can sniff out this data, intercept the stuff that looks interesting, which can be done by reading the headers and footers and determining what the message/information contains, and decode it to view in plain text on their computer.

Think of this form of attack as a postman opening a bank statement letter, writing down all your bank details, then sealing the envelope before posting it through your door. The data packets are easily intercepted on the free Wi-Fi and unless you're using a HTTPS site, they take very little effort to decode and read.

Shoulder Surfing

Whilst not a technical way of intercepting data, hackers will still use the old tried and tested method of stealing information simply by sitting close to you and peering over your shoulder whilst you enter login details or write an email.

It doesn't take much skill, as we're usually so busy concentrating on other things that we often fail to notice someone looking over our shoulder. However, it's a real and credible threat, so be wary.



Fake Wi-Fi

This is another element to a MITM attack, also known as an Evil Twin. Essentially a hacker can sit at the same café as you and everyone else and use a set of tools that can pretend to be the actual Wi-Fi router belonging to the café. This enables them to do several things: first, they're able to beam out the fake Wi-Fi signal to every device within range, which in turn (if the users have their devices set to attach to any freely available Wi-Fi) will instantly connect to the fake signal. Secondly, once they have a device connected, they're able to use their laptop and the tools therein to intercept all the traffic that's being sent to their fake Wi-Fi signal. Thirdly, the attacker can connect themselves to the actual café Wi-Fi and act as a filter to the real connection to the Internet. The victim isn't even aware that their connection is compromised.

Naturally, this means that every single scrap of data is being filtered through the hacker's system. It's just up to them to collect it all, decode it and use the information within for their own gains.

Fake Sites

We've mentioned fake websites previously. This way of data interception is often working hand-in-hand with the scenario we're using as an example. Combining the aforementioned Evil Twin and packet sniffing methods, a hacker, who has taken the time to set up the scam, can create several fake website front ends that mimic banking sites, Outlook access, login pages and so on. They then host those sites on their interception laptop, together with the Evil Twin fake Wi-Fi and should a user connect and request the page of their bank they instead get the fake site that the hacker set up.

The victim will then unwittingly enter their details, which will be stored by the hacker before forwarding the victim to the actual bank website. The victim will then be required to re-enter their banking details into the actual bank website.

For their part, they simply think they're mistyped a password and gain access to their account as normal. Sadly, the hacker now has plain text information regarding all their login details and can begin to transfer money from their account.



10 Tips to Protect Yourself Against Interception

While it may seem like fearmongering, detailing the ways in which data can be intercepted, it's sadly a real world fact. Public Wi-Fi, hotspots and free access points are the bane of the security industry. Thankfully, there are ways in which you can protect yourself.

Public Safety

Despite the different and varied ways a hacker can gain access to your inbound and outbound data, there are means in which you can defend yourself. Here are ten tips to help you protect your data from being intercepted.

TIP 1 Not all public Wi-Fi access points are havens for nefarious hackers but that doesn't mean you should let your guard down. Every security software and firewall in the world can't help you if you're not savvy when it comes to information security. If you're going to use public Wi-Fi, don't use it for banking or other highly personal detail transactions.



TIP 2 It may not always be possible to spot an Evil Twin fake Wi-Fi access point. It's often best to double-check with members of staff, if it's a café, airport, restaurant or similar, that the Wi-Fi you're connecting to is actually theirs and not one that's being spoofed. Avoid Wi-Fi names like 'Free Wi-Fi Here' or similar.



TIP 3 Always double-check a website for spelling errors, older logos or anything else that may raise an alarm. If your banking website looks even remotely different from when you last used it, try and avoid logging into it until you get to a more secure Internet location.

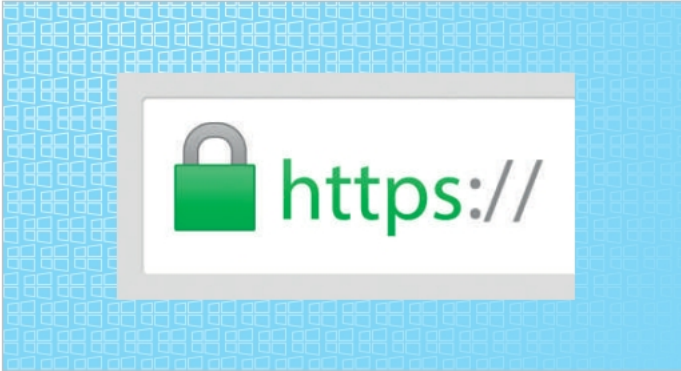


TIP 4 Ensure you use the latest antivirus and antimalware definitions for your security client. If you're going to use public Wi-Fi, make sure you're up to date prior to leaving, especially airport Wi-Fi points, and that the client is in good working order.

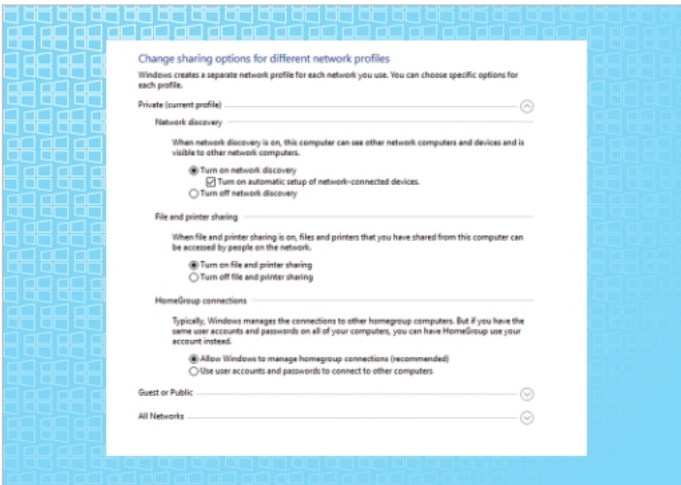




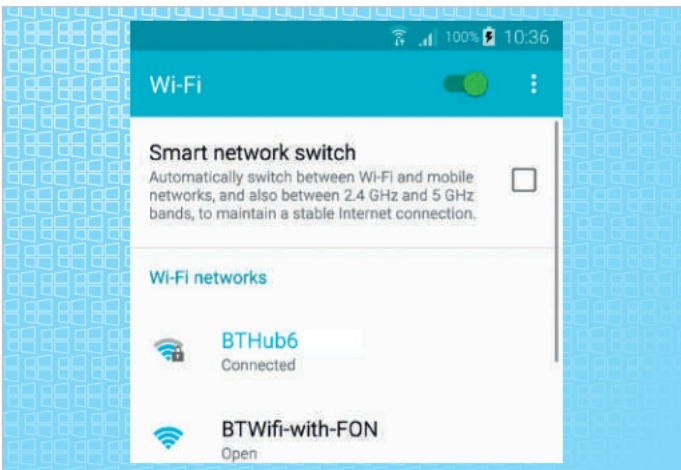
TIP 5 Always use HTTPS to access any website. This means that the information and data packets will be sent and received in an encrypted form and will make it exceedingly difficult for a hacker to decipher them. If possible, use an add-on such as HTTPS Everywhere for your browser of choice.



TIP 6 Turn off file sharing when you're using a public Wi-Fi access point. Whilst it's great to share your content on your home or work network, once you start using another network, your computer could start sharing that data with anyone who's also connected to the same network.



TIP 7 If you're not planning on using any public Wi-Fi points, then make sure that the Wi-Fi is turned off on your laptop, phone, tablet and other devices you have on you. There are instances when a device can automatically attach to any available network, unless otherwise told to.



TIP 8 Using a VPN when accessing a public Wi-Fi point is a fantastic way of protecting your data packets. They can still be intercepted but the VPN client encrypts all outgoing and incoming data with the highest possible levels, making it virtually impossible for a hacker to decode.



TIP 9 To avoid shoulder surfers, make sure that the area behind you is clear and enter passwords etc. via your keyboard in the same way you'd protect your card details in an ATM. Cover your keyboard as much as possible and make a point of looking around to make sure no one is watching you over your shoulder.



TIP 10 If possible, always use a two-factor form of authentication. For example, some banks will utilise both a login from their website as well as a text sent with a unique code to a registered phone number. This way you ensure that the banking site is legitimate and a hacker can't go any further without the SMS pin sent by the bank.





How to Secure Your Devices

Mobile device hacking is on the rise. Most people now carry a phone or tablet around with them all the time, containing their emails, browser data, photos and enough personal information for someone to be interested.

Ten Tips for Safer Mobiles

Your personal information is worth quite a bit to the right group of people. It's not just Windows security you need to keep in mind, you need to consider your mobile security too.

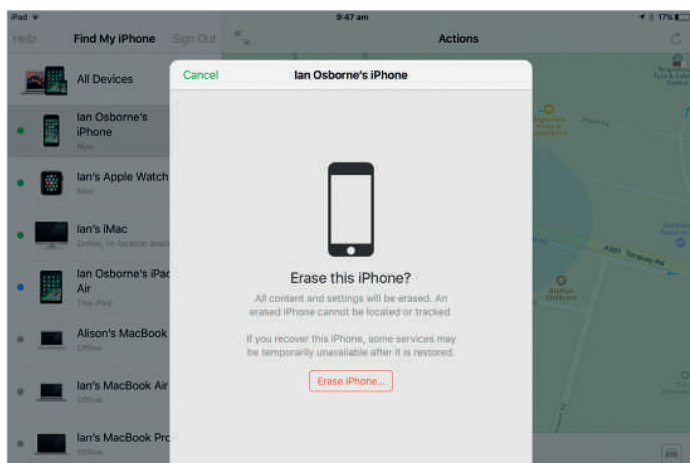
SECURITY LOCK

Locking your device is one of the most basic of security tips for mobile devices. Either use a number code, pattern lock or finger print to lock your device when not in use. Should someone steal it, it becomes a little more difficult for them to gain access. That won't stop a professional digital criminal, but it will deter the rest.



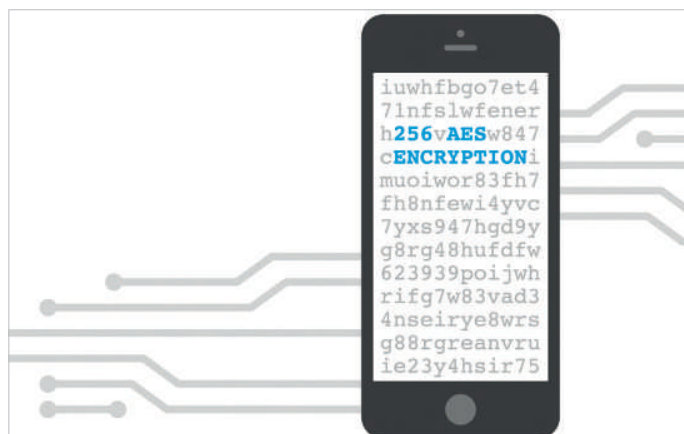
REMOTE WIPE

If possible set up some form of remote wipe. Should your phone or tablet be stolen or lost, you'll be able to use another Internet connected computer to send a delete signal to the lost device. You may never see the phone again but at least the personal data within is now out of the hands of others.



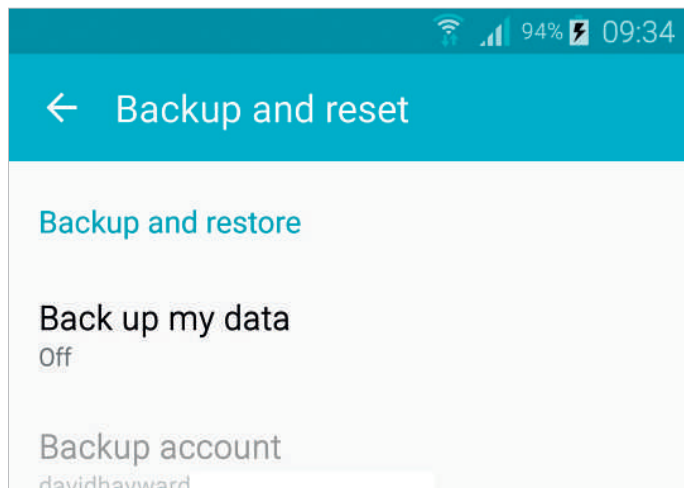
MOBILE ENCRYPTION

It's possible to set up data encryption on mobile devices these days. For example, you can encrypt the entire device or just the part that contains emails and personal or banking data. Either way, encryption will protect the contents of your device.



BACKUP DATA

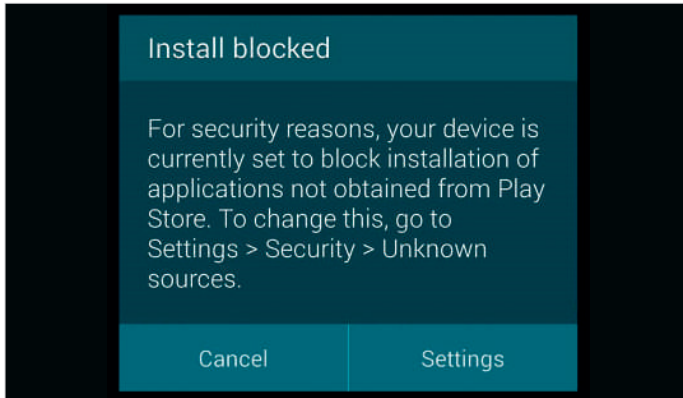
Make sure that the data you have on your device is regularly backed up. You may have umpteen security elements in place but if the device is lost and you haven't made a backup, then your data is lost too.





BLOCK INSTALLATIONS

Try to avoid installing third-party apps. iOS devices are covered in this regard thanks to Apple's walled garden approach to its app store. However, Android users are particularly vulnerable. Don't install anything from an unknown source and research plenty before installing anything.



NO ROOTING

Avoid jailbreaking or rooting your device. Whilst it's regarded as a positive process, to remove the built-in software from the manufacturer and give you control over the device, it often also opens your device to backdoors that were previously sealed. Unless you know how to properly secure a device, leave rooting alone.



UPDATE SYSTEM

Keep your system as up to date as possible. It can be a pain having to frequently accept update and upgrade messages from your device, and waiting for the OS or the app to update itself, but more often than not an update will provide much needed security patches.



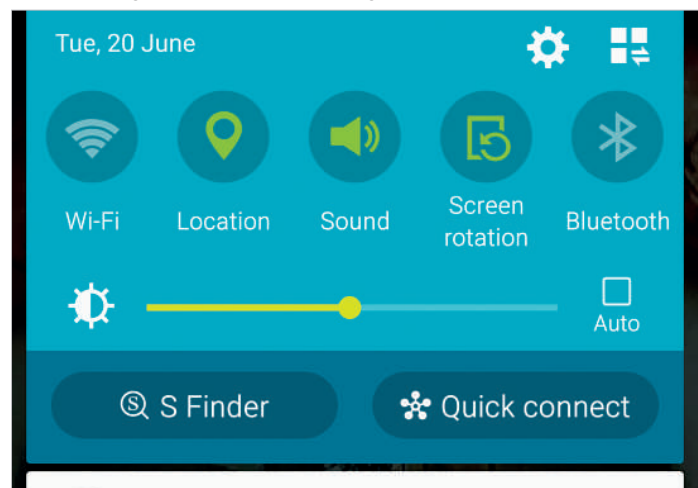
FALSE TEXTS

Be aware of social engineering phone scams, Vishing and Smishing in particular. Criminals love sending false banking texts, links to fake websites and all manner of other scams designed to gain access to your personal information.



POWER OFF WI-FI

Remember to turn off your Wi-Fi when you leave the home or office network. If you desperately require Internet access and don't want the data charges, then consider using a VPN if you're connecting to public Wi-Fi points.



MOBILE AV

Download and install a good mobile antivirus and malware tool set. Bitdefender, McAfee and all the other major security companies offer a mobile version of their products and with it you'll be better prepared for any potential cyber attack.





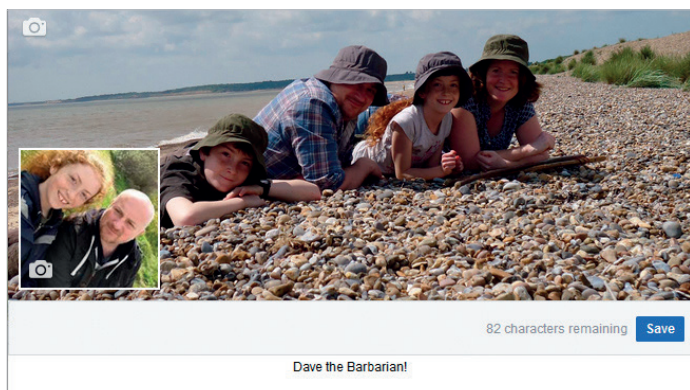
How to Secure Yourself on Facebook

Facebook has become one of the best sources for cyber criminals to gain personal information on the Internet. Without realising it, a user is giving out reams of data and in most circumstances they're making it public.

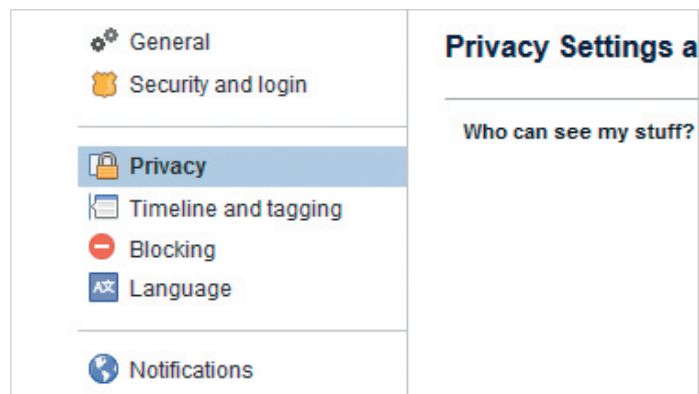
Tips for Better Facebook Profiles

The dangers of social media aren't just for young people, many adults have been duped into befriending someone they don't know and exposing their personal information.

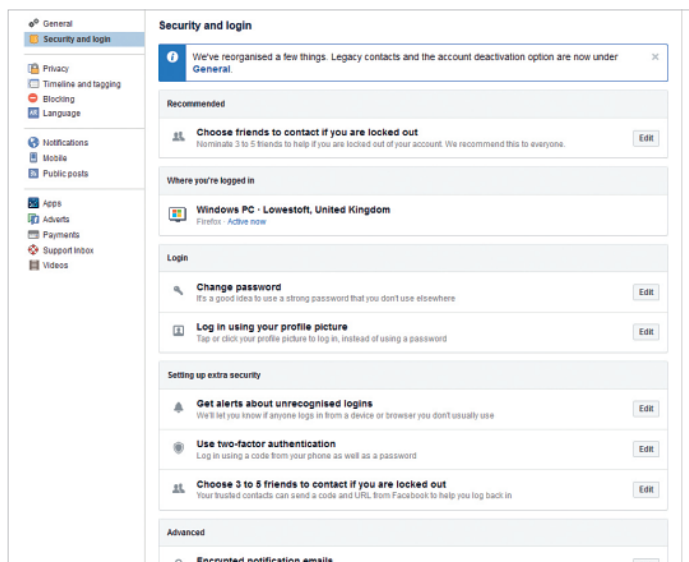
f Facebook's policy forbids the use of fake names but it does allow nickname names to be used. Where possible, use your nickname instead of your real name. This will effectively hide your real name details from those who would wish to exploit it.



f Go to Settings > Privacy, and make sure that the Who can see my stuff section is set for just friends, as opposed to friends of friends or public. This will effectively hide your Timeline contents from others and only your confirmed friends will be able to see any updates.



f Set up two-factor authentication, alerts about unrecognised logins and make sure that emails from Facebook are encrypted. These can all be found in the Settings > Security and Login section.



f Never post any contact information on your profile. We often automatically start filling in the phone number field on a site but take a moment to consider what the ramifications could be should your number be made aware outside your circle of friends. That also includes house address too.

Mobile Settings

Activating allows Facebook Mobile to send text messages to your phone. You can receive notifications for friend requests, messages, wall posts and status updates from your friends.

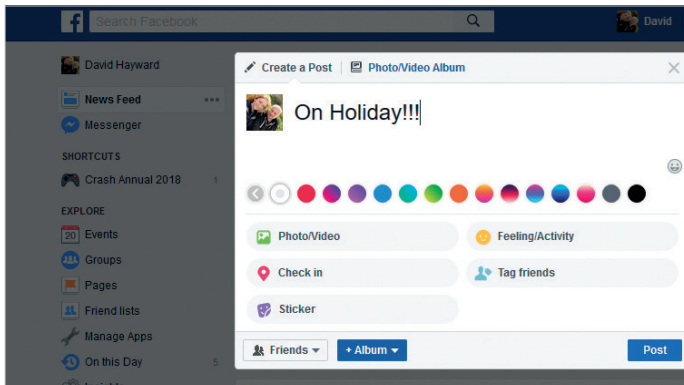
You can also update your status, search for phone numbers, or upload photos and videos from your phone.

[+ Add a phone](#)

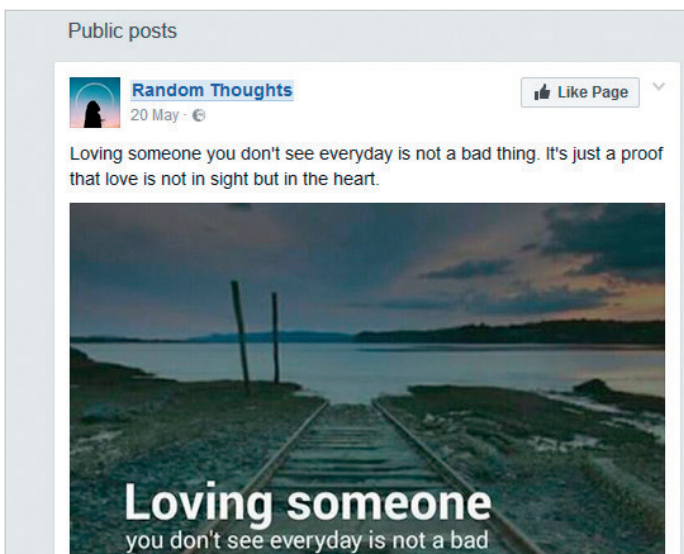
Learn more about using Facebook on your phone at [Facebook Mobile](#).



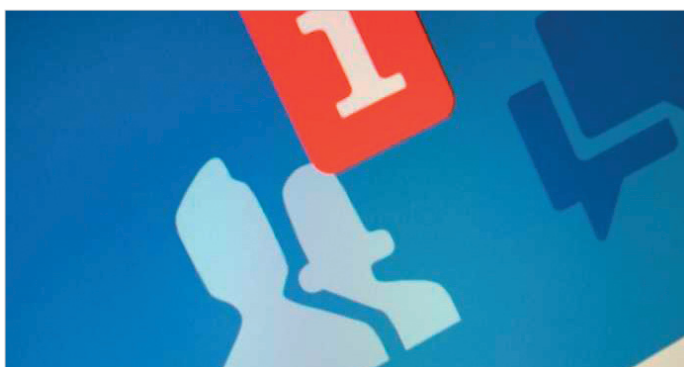
f Tempting as it may be, try to avoid posting your location. Whether you're at home alone, or you're on holiday, should that information be made available then a criminal will know that your house is empty or worse, that you're alone in it.



f Try and avoid sharing random thoughts of the day, inspirational quotes, fake news or other such items that appear on your Timeline from others. Often these instances are created to farm for shares and likes and as such can often be traced back to individuals who are simply looking for active Facebook accounts.



f Try not to accept every friend request you get. Take a moment to check the person out and if necessary message them to find out who they are and how they know you. If their comment is something like 'we met at the bar last month' then it's best to ignore the request, as they could be fishing for information.

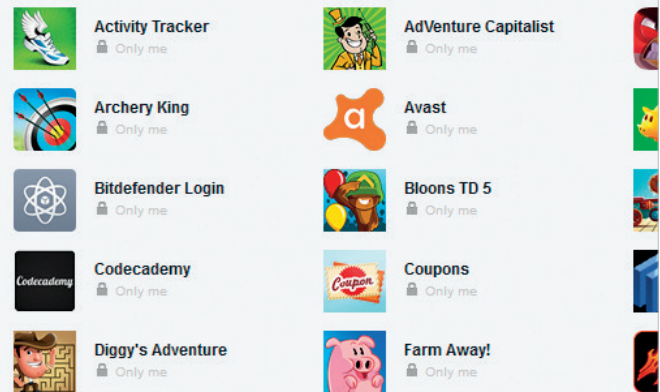


f Not all apps you install on your phone or tablet are good. Take a moment to read what an app will try to access when it's installed. Often a rogue app will attempt to access your Facebook account to farm for your and your friend's information.

App Settings

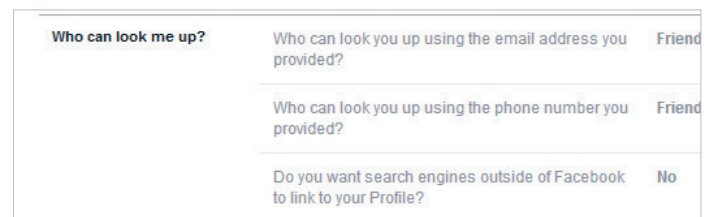
Logged in with Facebook 46

On Facebook, your name, profile picture, cover photo, gender, networks, username and user people and apps. [Learn why](#). Apps also have access to your Friends list and any information

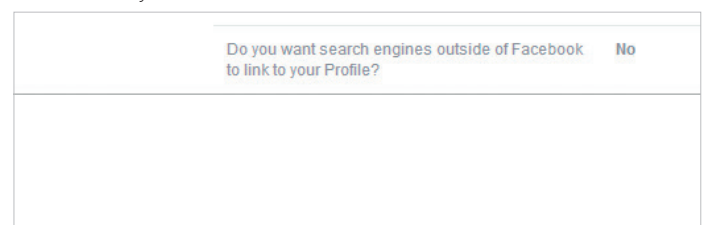


[Show all](#)

f Whilst in the Settings > Privacy section, consider editing the default options for the Who can look me up fields. These will prevent the public, or even friends of friends, from being able to find you on Facebook, which in turn adds a higher level of security to your account.



f Finally, ensure that the Do you want search engines outside of Facebook to link to your profile option is set to No. This will hide you from someone who has entered your name into Google in the hope that they might be able to find your Facebook account.





How to Secure Yourself on X FKA Twitter

X formerly known as Twitter's success has boomed in recent years. Where once it was simply one of the more popular social media platforms, thanks to presidential candidates and scores of celebrities, it's fast become the modern media phenomenon.

Securing the X-verse

Sadly, due to its popularity, Twitter is a hotbed of scammers, spammers, hackers and social engineers scouting out the next potential victim for monetary gain, or simply behaving abusively. Here are ten tips to help secure your Twitter account.



If you click on your profile picture and choose Settings and Privacy from the menu, you're able to set up a form of two-factor authentication called Verify Login Requests. This will enable Twitter to use your phone number to send texts for any login requests. So even if your password is compromised, the hacker can't get in without the text code.

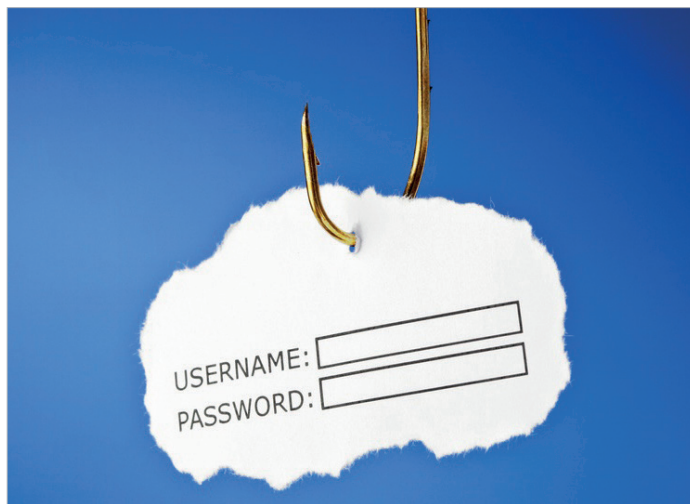
Security

Login verification ☐ Verify login requests.
You need to [add a phone number](#) to your Twitter account to enable this feature.

Password reset ☐ Require personal information to reset my password
When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.



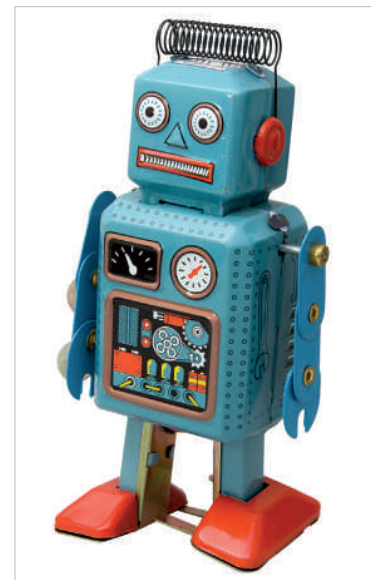
Just like most other social media platforms, phishing scams are rife on Twitter. Be wary of anyone sending you Tweets claiming to be someone you know, offering a too-good-to-be-true job or even informing you that your account is compromised. It's likely a phishing scam, so delete and report the instance to Twitter.



We've previously mentioned the fact that using weak passwords is, unsurprisingly, not recommended. However, you'd be amazed at how many people still use the likes of 'password1234' or something similar. Set a good, strong password that will take some cracking.

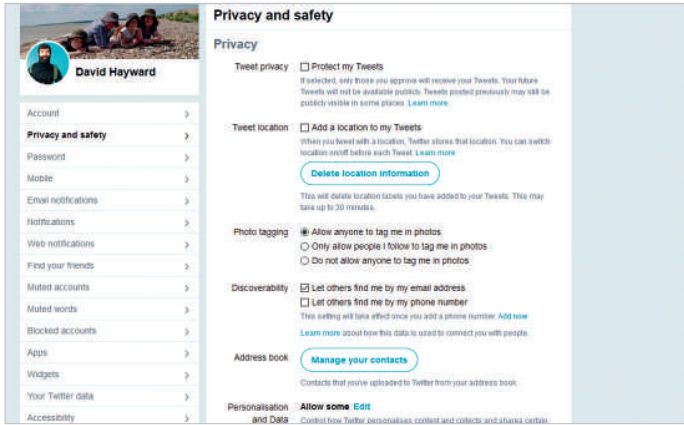


There are many accounts on Twitter that simply aren't real. These bots, as they're known, can be programmed to post daily amusing, inspiring and socially acceptable Tweets. On the flip side, other bots are designed to Tweet suspicious links to virus-infested websites. In short, unless you trust the account, don't follow any links.

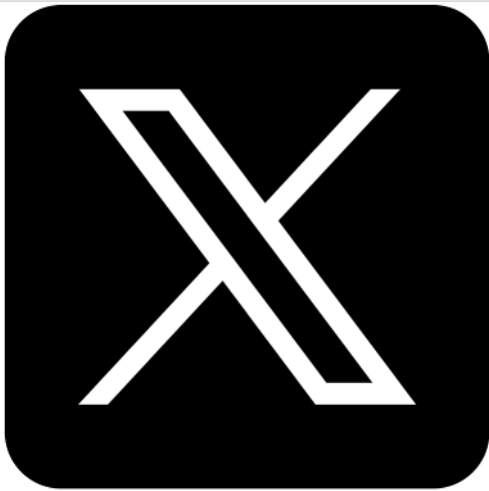




Within your account settings, you'll see a menu to the left with a Privacy and Safety option. Click this to enable Twitter privacy, Discoverability, Direct Message notifications, the ability to hide sensitive Tweets and the removal of blocked accounts. It's worth going through the list to further secure your account.



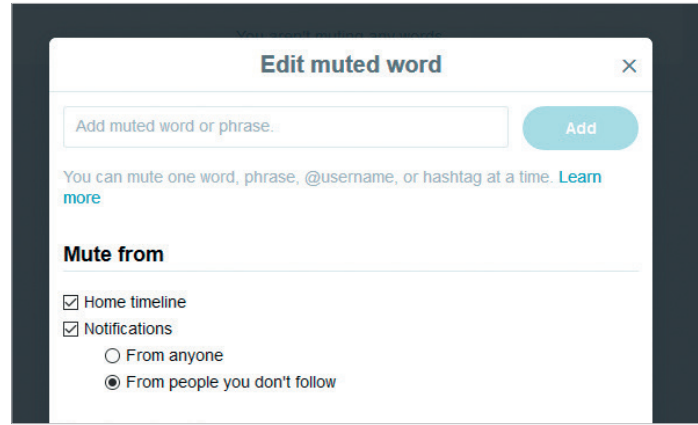
Direct messaging in Twitter is both advantageous and dangerous at the same time. Whilst great for communicating directly with another user, it's also used by others to lure in victims or send links to malicious websites. It's best to ignore most messages unless you know who they're from.



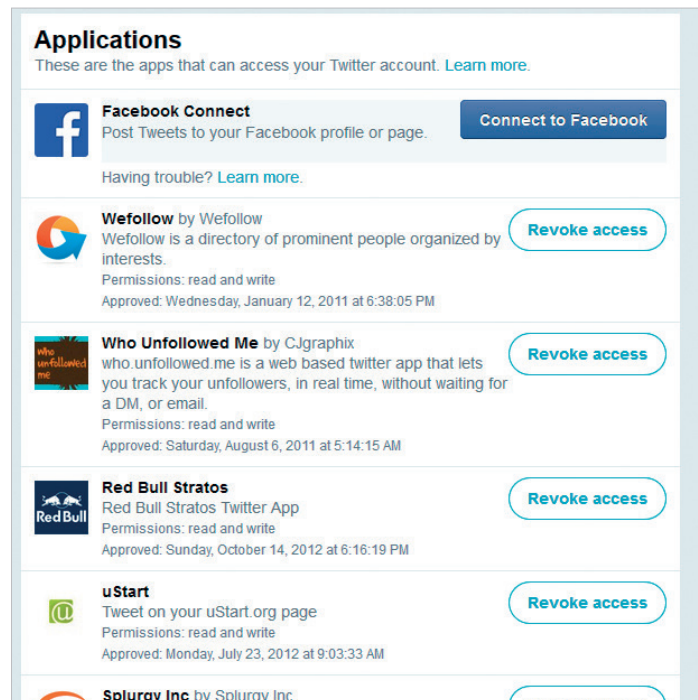
If you use your Twitter account to login into any third-party apps or games, then you may need to consider setting up a secondary Twitter account. Whilst convenient, some apps can be hijacked to collect account details, leaking them to hackers.



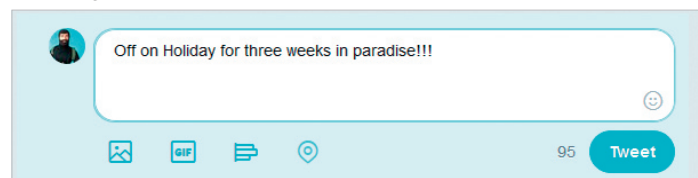
Word Muting is an excellent feature within Twitter's account settings. With it you're able to mute any words you don't want to see in your notifications or timeline. There are often Tweets you'd like to avoid even seeing in your timeline, so muting them is an ideal solution to help keep your account clean and free from negative aspects.



It's always worth browsing through the Apps section in the Twitter options. This is where you can allow or revoke access for any apps you've used via the Twitter account; and you can also see what rights each app has to your Twitter account.



Like Facebook, be careful of what you post. It's nice letting others know you're off on holiday to the Bahamas for several weeks but there could be a rogue account that's now informed of an empty house; and if you were foolish enough to mention your address in previous Tweets, they know exactly where to go.





How to Secure Yourself on WhatsApp

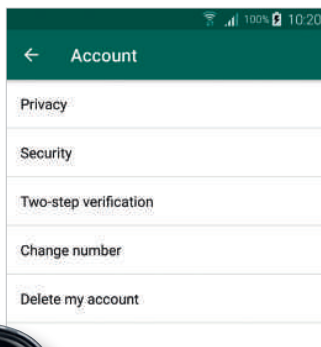
With over a billion users worldwide, WhatsApp is proving to be a force to be reckoned with in the social media marketplace. This messaging app was released over eight years ago and developed by the Facebook team; since then it's become the most popular messaging app.

WhatsApp Security Tips

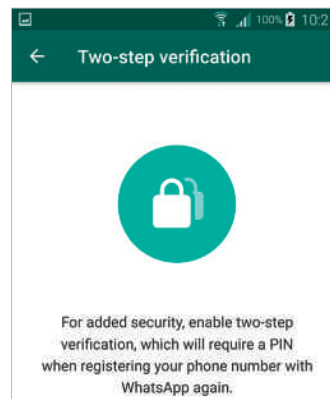
With this popularity comes a darker side to messaging. Accounts of terrorists using WhatsApp, along with hackers, scammers and all manner of nefarious individuals and groups are ever in the popular media.



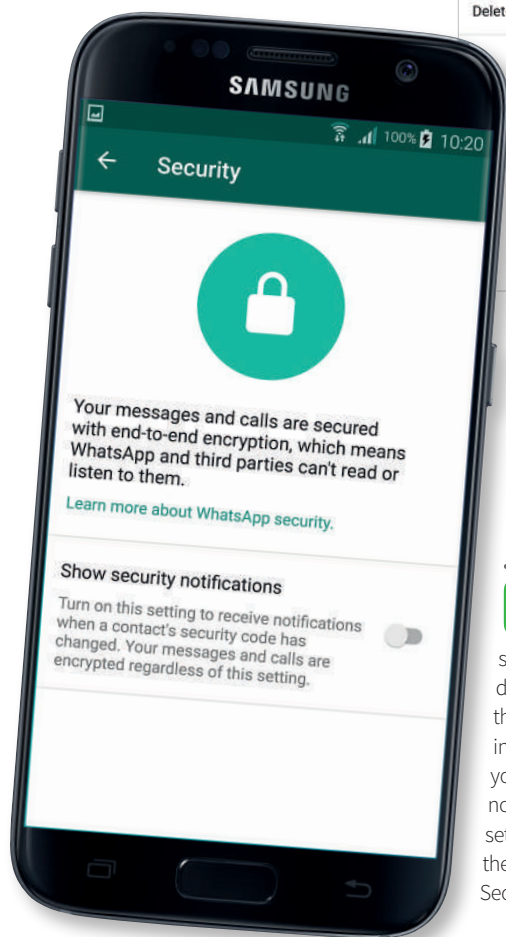
Protecting your WhatsApp account can be done mainly through the Settings > Account > Privacy option. In here you're able to secure your personal details, profile, status, messaging and who can see your account.



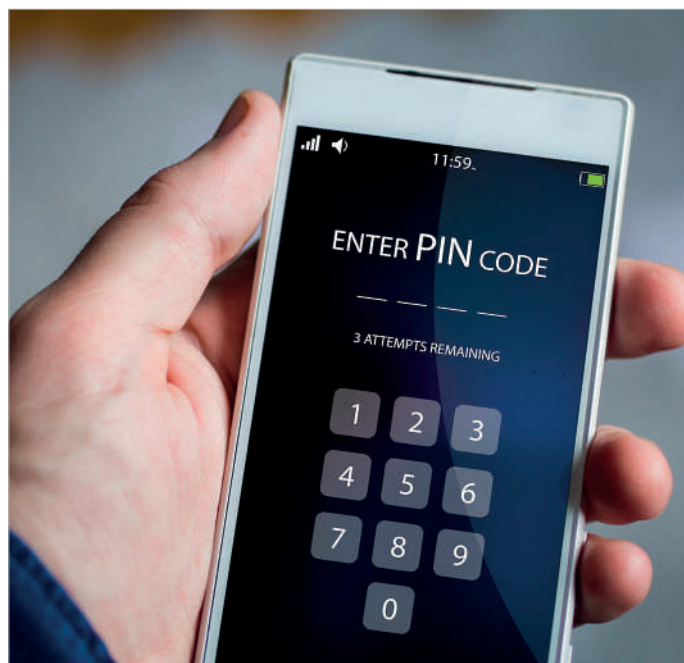
For added security you can opt for two-step authentication, which will require a PIN when registering your phone number with WhatsApp. This is an absolute must for those who use the app regularly.



Beyond WhatsApp itself, make sure that your phone or tablet is securely locked with an access PIN, pattern, facial or finger print recognition system. This way, should you lose your phone, it will be locked against anyone who tries to access it and WhatsApp.



Thankfully, WhatsApp already encrypts and secures messages sent from one device to another. This means that your data can't be intercepted and read. However, you can opt to view security notifications if a contact's security setting has been altered. This is in the Settings > Account > Security menu.

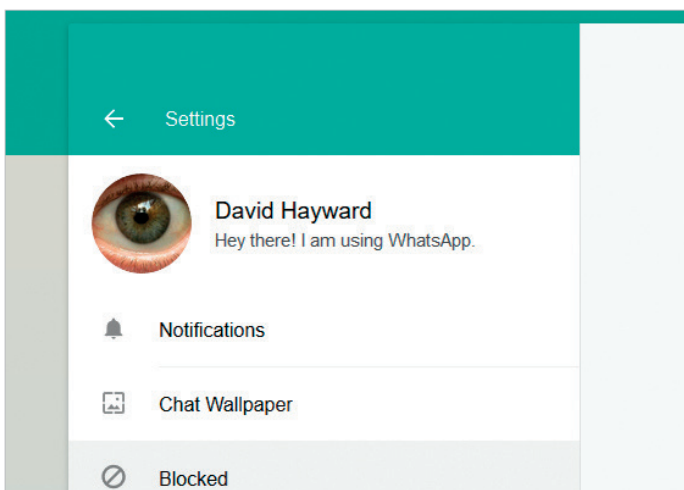




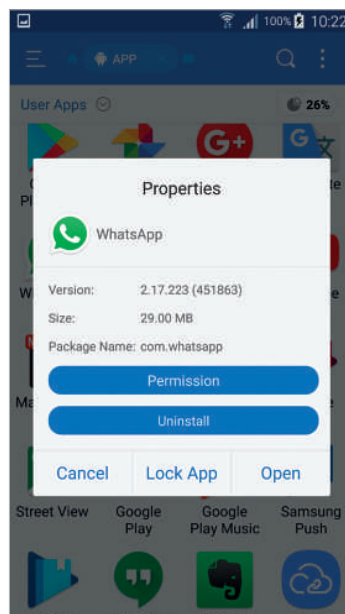
Generally you're not able to add users to your chat list if you don't already have them in your contacts list. However, clever phishing scams can have a victim add a contact, who can then message them using WhatsApp; as with all social media platforms, be wary of phishing attacks.



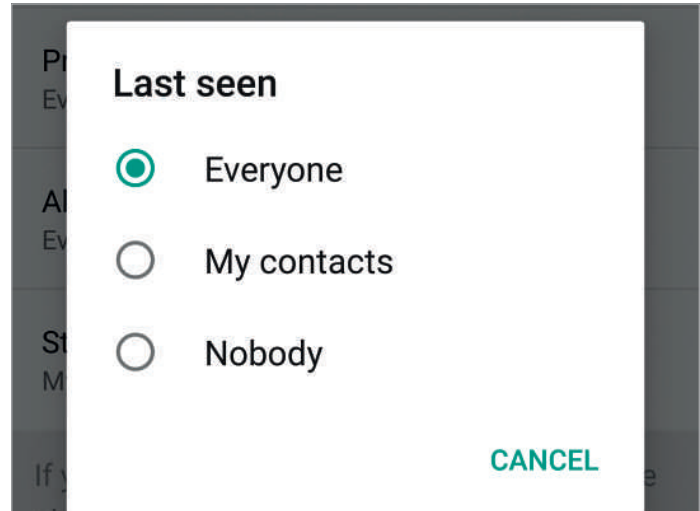
You can block users via the WhatsApp Web feature. Log into WhatsApp Web, and click on the three horizontal dots by your profile picture. Then click Settings and from there the Blocked option. You can select contacts to block from WhatsApp.



You can block all images from appearing on your photostream within WhatsApp. iOS users can look to their Settings then Privacy > Photos and deselect WhatsApp from the list of allowed apps. Android users will need to create a file called .nomedia within the WhatsApp images folder to stop the app from listing pictures.



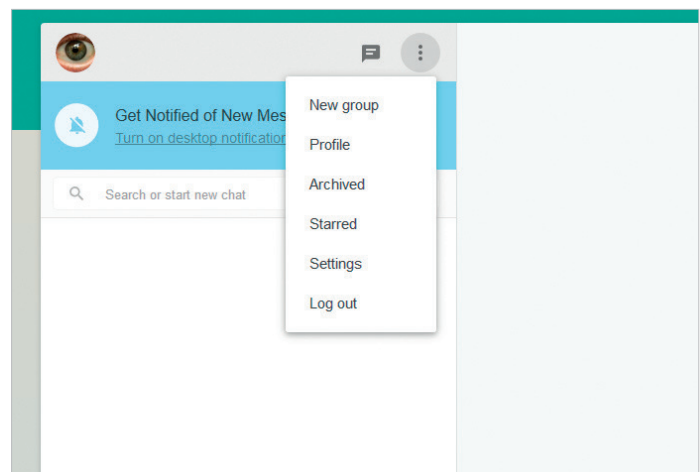
If you don't want WhatsApp contacts to see where you've been, you need to disable the Last Seen option within the Privacy settings. This will prevent other users from 'seeing' your movements. Should a malicious contact be added, they will never know where you are or have been.



Be wary of scams where you're contacted through other social media accounts informing you that your WhatsApp account has been compromised. These often request you to add a so-called legitimate contact, who in reality isn't, or visit a webpage that's riddled with malware.



If you use WhatsApp Web it's always best to ensure that you've logged out of it correctly before leaving your computer. The last thing you need is for someone to come over to your computer and view any conversations between contacts.



What to Avoid when Creating a Password

Creating a strong password sounds easy on paper but when you're presented with the password box it's easy to become stumped. Should you get past that part, there are also security rules to follow to further protect that password.

PA55W0RD1234

To help you create the perfect password, and secure it further, here are ten tips for happier password management. There's always password pitfalls but stick to these general tips and you should be okay.

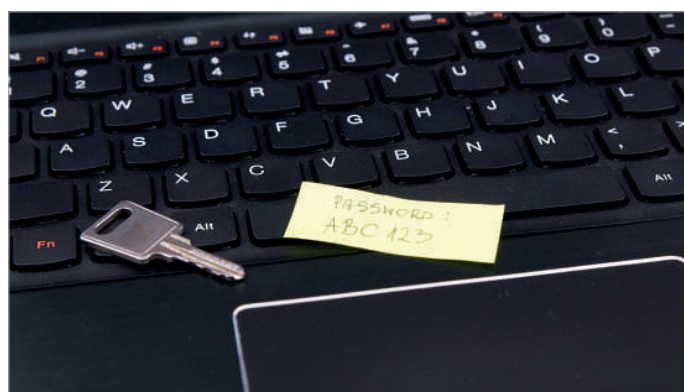
OBVIOUS DATES

Never use your date of birth, partner's date of birth, children's date of birth, pet's names, family names grew up in. This is all information that can easily be sites or even a clever Internet search.



VISIBLE PASSWORD

Never write your password down on a Post-It note or somewhere near your computer. It's a bad idea to visit your computer whilst you're on a coffee break.



SAME PASSWORDS

SAME PASSWORDS Never use the same password for multiple sites. It's tempting and easy to have a single password for everything but should that password ever become compromised you will lose access to every site you visit, including any banking sites.



COMMON PASSWORDS

COMMON PASSWORDS

Try and avoid using common words in your password. Most password attacks are brute force, using dictionary words to gain access. Avoid using sequences of numbers, such as 1234. Instead, try inserting numbers, capital letters and symbols into words, such as C0m"0 instead of the word common, for example. However, avoid common words altogether if possible.



**CHANGE REGULARLY**

Regularly change your password. Most companies and good sites will require you to enter a new password that hasn't been used previously in the last few months every thirty days or so. If not, then you should actively keep changing your password yourself.

UNTRUSTED DEVICES

Never enter your password on a device or computer you don't trust. Entering your account details on a public computer, such as a kiosk or library, is dangerous as you don't know what protection these machines have nor whether they've already been compromised.

**PUBLIC WI-FI**

Try to avoid logging into certain sites when you're using public Wi-Fi. We've already covered how data on a public, free Wi-Fi access point can be intercepted. Your passwords, therefore, can be intercepted and viewed in plain text by a hacker.

**LENGTHY PASSWORDS**

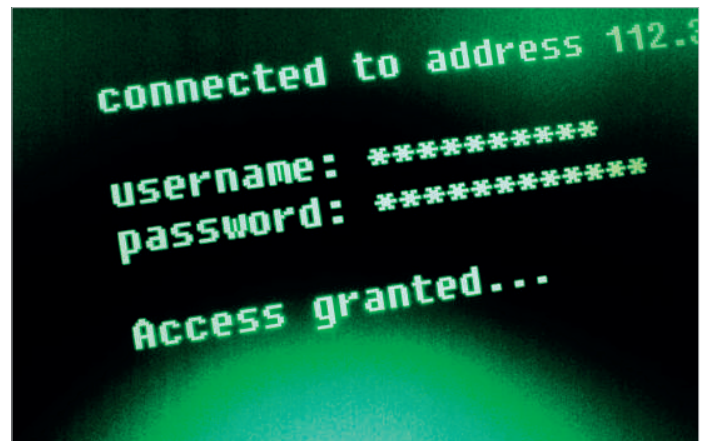
Don't use short passwords. The longer they are, generally, the harder and more complex it will be should anyone try to crack it. A longer password that also utilises upper and lower case, numbers and symbols can't easily be viewed by any shoulder surfers.

**SECURITY QUESTIONS**

In addition to creating a password, some sites also offer a rescue security question. Sadly most of these questions are a little too easy to get the answers for. Questions such as Mother's Maiden name, first pet, town where you grew up, etc. can again be obtained by the clever hacker.

STRONG PASSWORDS

A strong password isn't going to be easy to remember at first. For example, something like 8%&KY4&\$XzwMhfrk will take a hacker around a hundred thousand years to crack but it hardly flows off the tongue. Find a happy medium and make your password as strong as possible.





Password Generators and Tools

We've looked at some tips on what not to include when coming up with a strong password. However, it's not always as straight forward as that. Whilst some can come up with an elaborate and incredibly strong password, others struggle. Thankfully, there's help on offer.

Top Ten Password Generators

We live in an age where you don't have to sit with a dictionary and cryptic decoder to come up with an excellent password. There are many generators freely available to help you out. Here's our top ten.

NORTON IDENTITY SAFE PASSWORD GENERATOR

Norton by Symantec, offers a handy free password online generator. You can set the password length, include letters, mixed case, numbers, punctuation and no identical characters. You can find it at:

<https://identitysafe.norton.com/password-generator/>.

WIGHT HAT PASSWORD GENERATOR

This online password generator has been

around for quite some time and has proved to be one of the best available for those after a unique and unbreakable password. There are ample options, and none of the passwords generated are stored remotely. Visit:

<http://strongpasswordgenerator.org/> for more information.

STRONG PASSWORD GENERATOR

Another great online resource that will create

an incredibly strong password based on the options you choose. You can choose the length, punctuation and avoid similar characters but also display phonetic words to make it easier to remember. Try it out at:

<https://strongpasswordgenerator.com/>.

LASTPASS

LastPass is a popular password management program, which we'll look at in the next section; it also offers a free password generator. Found at <https://lastpass.com/generatepassword.php>, this excellent tool will help you create a strong and virtually unbreakable password in seconds.



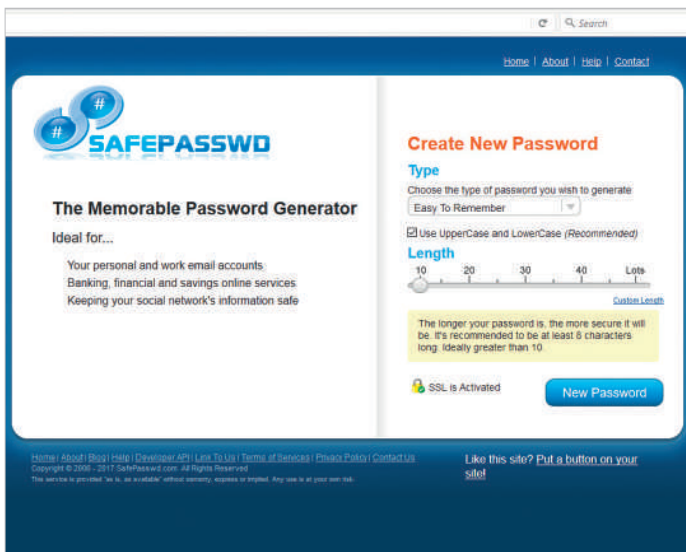
MSD SERVICES

An interesting site this, one that will allow you to create multiple unique passwords, based on length, upper and lower case, number and symbols as well as whether the end result will be pronounceable or completely random. It's at <https://msdservices.com/apg/index.php> for those after several passwords.



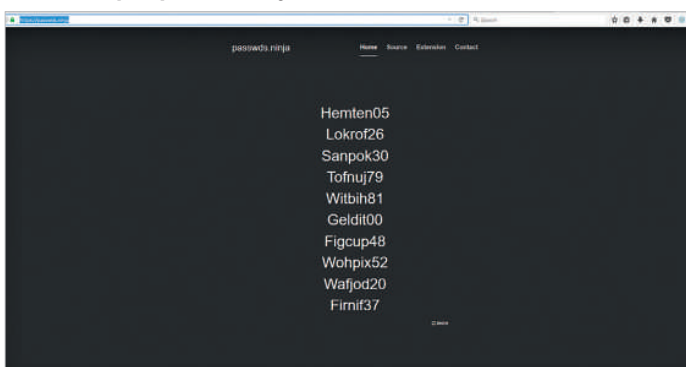
SAFEPASSWD

Another great site to have in your password arsenal. SafePasswd has been around since 2006 and is regarded as one of the best online password generators. The options are many and with them you can create something truly impossible to crack. You can find it at: <https://www.safepasswd.com/>.



PASSEDS.NINJA

This is a quick and easy online password generator. You won't get any options or added extras, you simply click a button and ten unique passwords will be displayed for you to choose from. It's worth looking into for a quick solution to password creation; <https://passwds.ninja/>.



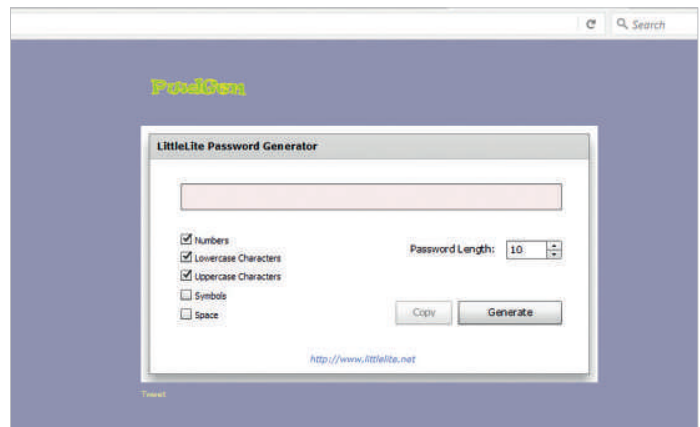
XKPASSWRD

This site is powered by the XKPasswd.pm Perl module, which offers a range of settings to help create a unique and very strong password. There are plenty of options to choose from and you can save and load your preferred configuration for later. It's at: <https://xkpasswd.net/s/> if you want to check it out.



LITTLELITE PASSWORD GENERATOR

Another simple but easy to use and good online password generator. LittleLite offers some options, including password length, number, upper and lower case, symbols and spaces. It's found at <http://www.littlelite.net/pwdgen/> and certainly worth considering bookmarking.



DINOPASS

For kids at school or when online, DinoPass is an excellent resource that will help them come up with a memorable, yet strong password. You can choose between a simple or strong password type, depending on where it's going to be used and there's meanings of each to help out, too. You can find it at: <http://www.dinopass.com/>.





Top Ten Password Managers

Creating uncrackable passwords is one thing, remembering them for each of the services that require one is something else entirely. The reason why most people opt for a single password for all their accounts is simply due to not being able to remember them all. This is where password managers help.

Manage Those Passwords

Password managers differ in what they offer, how they work and what optional extras they provide. Therefore it can be tricky to find one that fits the bill. Some are free, others cost a monthly or annual fee; here are ten to consider.

LASTPASS

LastPass, which also offer a free password generator, is regarded as one of the finest managers available. There's a free version that offers unlimited password storage, cross-platform access, two-factor authentication and elevated levels of encryption. There's also a Premium version that offers a lot more, including 1GB of encrypted file storage and higher levels of encryption.



STICKY PASSWORD

Sticky Password is available both as free or Premium versions, costing just £24 and offers two-factor authentication, autofill for websites, advanced biometrics; it's also available on all major platforms. The Premium version goes further with cloud backup and syncing and with every license purchased a Manatee is saved. Certainly worth considering.



ZOHO VAULT

Zoho Vault is another excellent password management application. With a free version on offer, moving up to Enterprise levels for just €7 per month, Zoho allows unlimited passwords, access from all platforms, password tracking, offline access, auto-login for websites and much more.



DASHLANE

With free, Premium and Business options available, Dashlane covers a huge user base. Its features are many and it offers the user a high degree of encryption and security alongside all the usual auto-filling, two-factor authentication and the ability to export data.



**KEEPER**

Keeper is a powerful and feature rich password manager that has Individual, Family and Business plans available for £20.99, £44.99, and £22 per year respectively. With unlimited password storage, unlimited device syncing, finger print login and secure cloud backup, amongst others, it's certainly one to consider.

**KEEPASS**

KeePass is a freely available, open source password manager that's regularly updated and comes with a long list of interesting features. You can import and export password data, it's fully portable so there's no installation required and it adheres to 256-bit AES encryption.

**1PASSWORD**

1Password offer an individual and Family plan for as little as £2.30 and £4 per year. With it you can access password across all your devices and operating systems; there's offline access, automatic syncing, 1GB of secure storage available and a 365 day password history recovery.

**PASSWORD BOSS**

Password Boss offers both free and Premium plans, with the Premium plan costing around £24 per year. There are ample features to enjoy, including cross platform support, full military encryption, cloud syncing and more.

**TRUE KEY**

True Key is an excellent password manager with a free and Premium plan available; the Premium plan costing around £29.99 a year. It's unique in that it utilises facial recognition as well as finger print, and integration with Windows Hello. There are plenty of other options available too, so it's worth looking into.

**LOGMEONCE**

LogMeOnce is an award-winning password manager that incorporates many interesting features. It's ultimate selling point, however, is a passwordless operation, whereby you are able to log in to any website or service just by using facial recognition. Prices do vary across the Premium, Professional and Ultimate editions but the personal version is free.





Shopping Online and Security

Windows is continually improving and as such the new updates have brought a more customisable degree of control over the operating system's privacy configuration; something that Microsoft has always been criticised for in the past.

The length of breadth of online shopping is far too vast to cover every conceivable angle here. So rather than

“

10 Online Shopping Security Tips

”

focus on particular elements, here are ten online shopping security tips to apply across the board.

FAKE SITES

Ensure that you're buying from a real website. Fake sites are remarkably easy to create by the clever hacker and are designed to steal your transactions. Be wary of sites other than the big names. While smaller online shops are fine, just look into the type of security it's using and do some research before purchasing.

RUSH BUYING

Don't be fooled into

rush buying something that's at a ridiculously low price. If a site is selling an iPhone for £20, then it's more than likely to be a ruse to lure you in and steal your money.

BOGUS EMAIL

Strange email addresses are

something to look out for with suspect online shops. If the support email or contact information for the site is something like: ebayhelp@gmail.com instead of support@ebay.com, then there's most definitely something wrong.

**USE HTTPS**

Remember to load up the online shop using HTTPS instead of HTTP. This will ensure that the transactions and data sent between you and it are encrypted to the highest possible levels. If possible, use a browser add-on such as HTTPS Everywhere.

STRONG PASSWORDS

Use a strong and unique password for all your shopping sites. Occasionally, although not often, websites can be hacked and the database of users is leaked. If your password is strong enough, it will stand up to any decryption methods.

AVOID PUBLIC Wi-Fi

Tempting as it may be, don't use a public Wi-Fi access point to conduct any online shopping. For one, you could be attached to an Evil Twin Wi-Fi point, where the hacker is filtering all information through their system and two, all your data can be intercepted and potentially read.

SHOPPING APPS

If possible, always use an online shop's dedicated app rather than the standard website. Websites can be compromised, however apps from iTunes and the Windows Store, for example, can't be altered by a third-party.

3RD PARTY SECURITY

Invest in one of the many third-party antivirus and malware suites, such as Bitdefender. These programs also offer extra security when shopping online and can help prevent any hacking or data interception from happening whilst the transactions are in progress. They can also check the site you're buying from, too.

PAYPAL

If possible use PayPal or a Credit Card as opposed to a Debit Card. Credit cards have an extra layer of protection and legal standing than that of a debit card; PayPal features many protection elements within its accounts too.

BANK TRANSACTIONS

Always keep an eye on your bank account and the transactions that go on after you've conducted online shopping. This will help you get an idea of what's going on and should something suddenly crop up that looks suspicious, then you're able to inform your bank before too much damage is done.



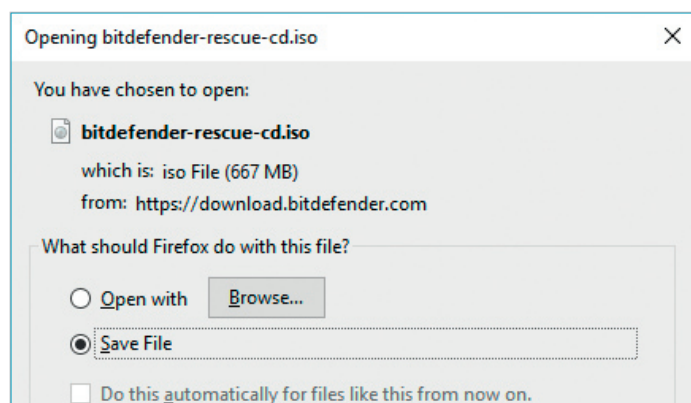
How to Remove a Virus or Malware from a PC

So far we've looked at ways to prevent getting scammed or indeed getting malware on your system but what if you're unlucky enough to already have some form of digital infection? Thankfully, there's a way to remove malware and viruses from your computer.

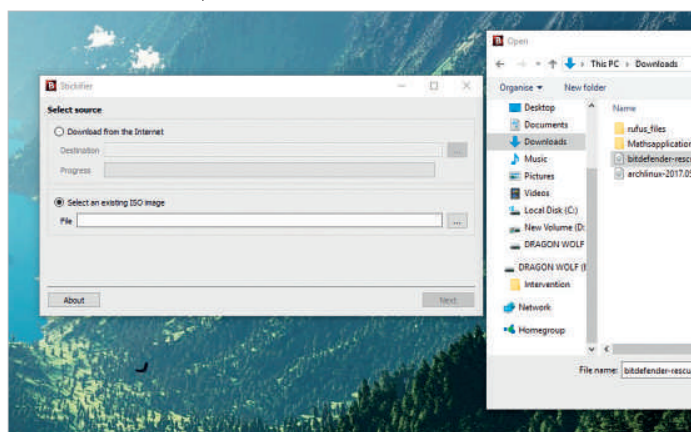
Malware Busters

For this tutorial let's use a preconfigured rescue disk from Bitdefender. You need to transfer, or burn, the disk contents to a CD or a USB stick and boot into the safe environment through one of those mediums.

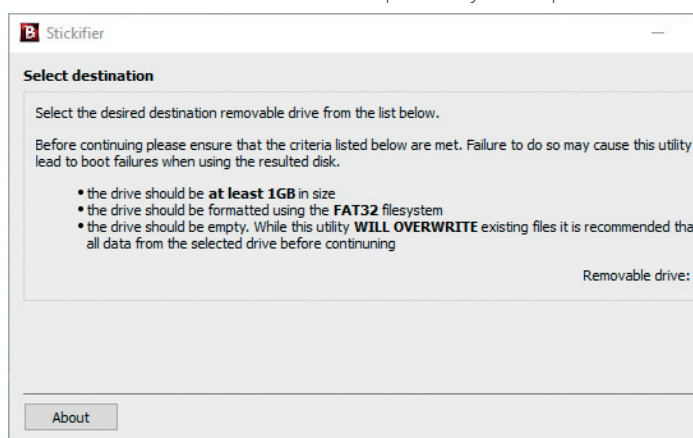
STEP 1 Make sure you have a blank CD or a USB stick that's at least 1GB in size. The Bitdefender Rescue Disk is downloaded as an ISO (which is an image file containing all the disk information) and can be downloaded from [www.download.bitdefender.com/rescue_cd/latest/bitdefender-rescue-cd.iso](https://download.bitdefender.com/rescue_cd/latest/bitdefender-rescue-cd.iso).



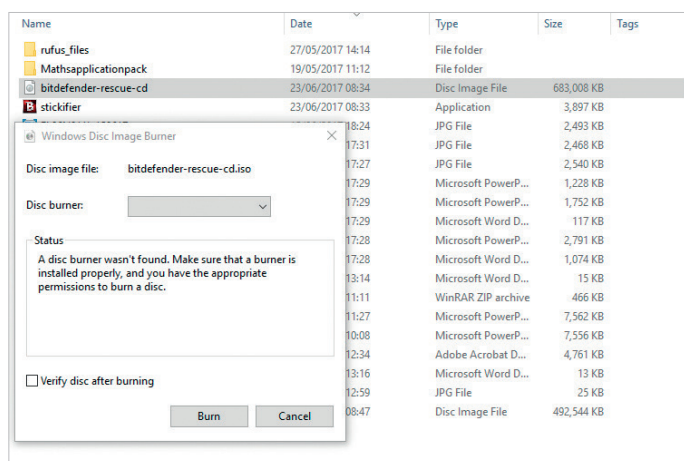
STEP 2 To transfer the ISO to USB download Stickifier, which is an executable that doesn't require any installation. Insert your USB stick and double-click Stickifier. Click the Select an Existing ISO Image option followed by the three full-stops and using Windows Explorer, locate the downloaded Bitdefender Rescue ISO. Click the Open button to select the image and continue with the process.



STEP 3 Click the Next button and using the drop-down menu next to Removeable Drive choose the drive letter of your USB stick. Click Next to start the transfer of the image. Once the image is transferred click the Finish button and remove the USB stick and power off your computer.



STEP 4 If you're using a CD, start by inserting the CD into the drive. Locate the downloaded Bitdefender Rescue ISO, right-click it and choose Burn Disc Image from the context menu. Tick the Verify disc after burning option and click the Burn button to start the process. Once the ISO is burnt to the disc, you can power off your computer.





STEP 5 You now need to allow your PC to boot up into the Bitdefender Rescue CD environment. Power up your PC and open the Boot Option Menu. This could be accessed by pressing F12, depending on the make and manufacturer of your PC motherboard. With the boot options available, select either the CD or USB stick and press Enter.



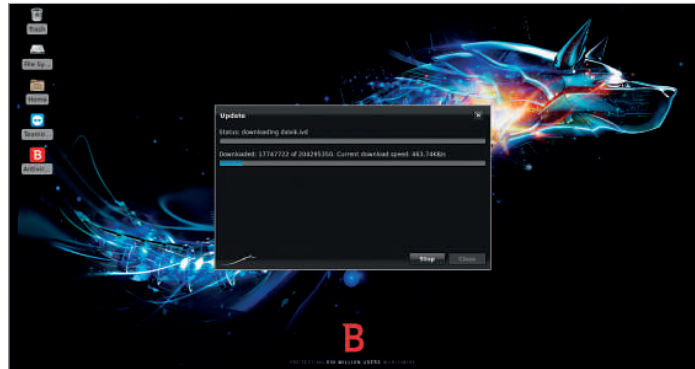
STEP 6 The PC will now boot into the Bitdefender Rescue Disc environment. This is a custom Linux operating system with all the necessary Bitdefender security tools preinstalled. First, you need to choose which language to load the environment. Use the arrow keys, and press Enter for your language choice.



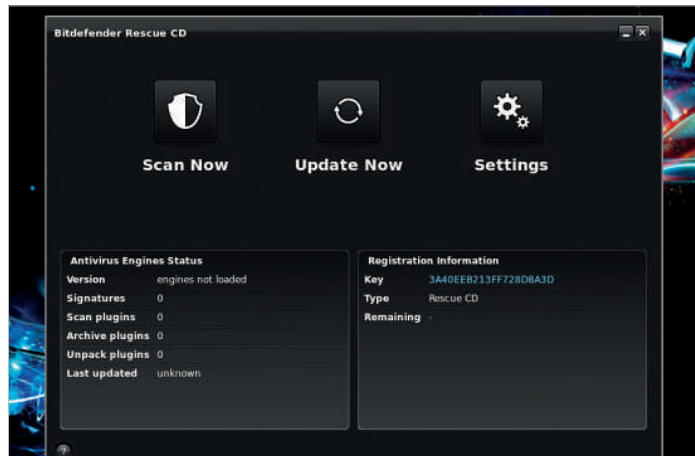
STEP 7 Ideally you should use a wired Internet connection but if you're on wireless, click on the network icon in the bottom right of the desktop to establish a connection with your router. Once you're connected to the Internet, double-click the red Bitdefender icon on the desktop, labelled Antivirus Scanner.



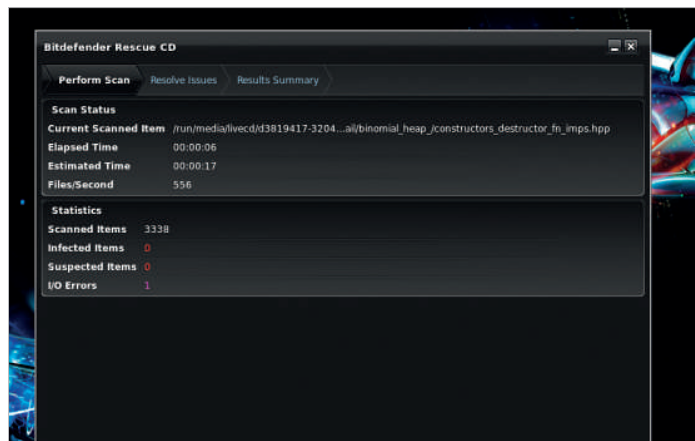
STEP 8 You need to accept the license agreement notification first. Tick the I agree box, followed by clicking the Continue button. The virus scanning software will then start to automatically update itself with the latest virus definitions from the Bitdefender servers. The process won't take too long, so let it run through the update.



STEP 9 Once the update is complete you're taken to the main Bitdefender Rescue CD antivirus interface. The three main options: Scan Now, Update Now and Settings are fairly self-explanatory; the Settings allows you to set a few more options regarding the scan, however the defaults will suffice.



STEP 10 To remove a virus on your PC, click on the Scan Now button. Select the drive you wish to scan and click the Open button to commence scanning the system. Any viruses found will be detailed along with options for removal. The process may take some time, so be prepared for a lengthy wait.





COMPLETE MANUAL SERIES

Stay tuned...

This issue has come to its end, thank you for joining on this adventure, don't worry as our journey together is just getting started. So don't miss out on our exciting next issue, coming in Summer 2026. Hit that Subscribe button as we have even more high quality professional tech support, tutorials and guides that you can't afford to miss!

Also From Papercut...

Why not check out these other amazing publications from the world leader in consumer technology bookazines, Papercut.



The Complete Manual Series:

Internet Security
26 | ISBN: 978-1-914404-56-6

Published by: Papercut Limited

Digital distribution by: Pocketmags & Zinio
© 2026 Papercut Limited All rights reserved. No part of this publication may be reproduced in any form, stored in a retrieval system or integrated into any other publication, database or commercial programs without the express written permission of the publisher. Under no circumstances should this publication and its contents be resold, loaned out or used in any form by way of trade without the publisher's written permission. While we pride ourselves on the quality of the information we provide, Papercut Limited reserves the right not to be held responsible for any mistakes or inaccuracies found within the text of this publication. Due to the nature of the tech industry, the publisher cannot guarantee that all apps and software will work on every version of device. It remains the purchaser's sole responsibility to determine

the suitability of this book and its content for whatever purpose. We advise all potential buyers to check listing prior to purchase for confirmation of actual content. All editorial opinion herein is that of the reviewer - as an individual - and is not representative of the publisher or any of its affiliates. Therefore the publisher holds no responsibility in regard to editorial opinion and content. This is an independent publication and as such does not necessarily reflect the views or opinions of the producers of apps or products contained within. This publication is not endorsed or associated in any way with Microsoft, Google, The Linux Foundation, Canonical Ltd, Debian Project, Lenovo, Dell, Hewlett-Packard, Apple and Samsung or any associate or affiliate company. All copyrights, trademarks and registered trademarks for the respective companies are acknowledged. Relevant graphic imagery reproduced with courtesy of Lenovo, Hewlett-Packard, Dell, Samsung, Linux Mint, Canonical, CyberGhost, BBC News, MINIX, Steam and Valve, Intel, AMD, Crucial, SanDisk, ASRock, CIT, Cooler Master, Nvidia, BenQ and Apple. Windows is a trademark of Microsoft Corporation, registered in the United

States and other countries. Windows 10 & 11 ©2024 Microsoft Corporation. Additional images contained within this publication are reproduced under licence from Shutterstock. Any images reproduced on the front cover are solely for design purposes and are not representative of content. Prices, international availability, ratings, titles and content are subject to change. All information was correct at time of publication. Some content may have been previously published in other volumes or titles.

 **Papercut Limited**
Registered in England & Wales No: 04308513

ADVERTISING – For our latest media packs please contact:
James Gale - jgale@pclpublications.com
or email - advertising@pclpublications.com
INTERNATIONAL LICENSING – Papercut Limited has many great publications and all are available for licensing worldwide.
For more information email: jgale@pclpublications.com



Papercut

www.pclpublications.com