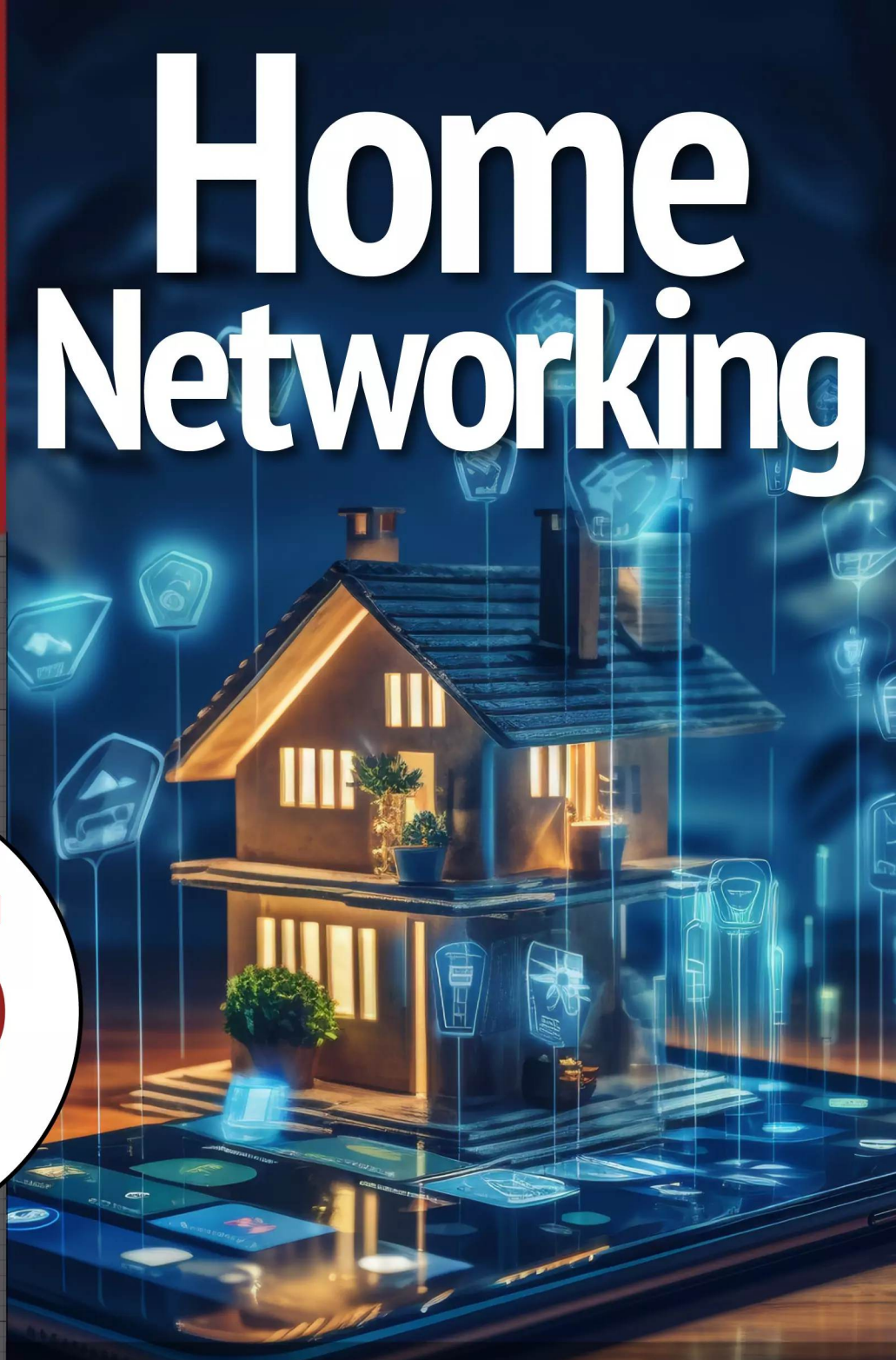
TRICKS & TIPS

Home Networking



- Essential tutorials, guides and tips for securely networking your home

OVER 465 SECRETS & HACKS

- Beat hackers, viruses and malware with our top security tips and advice
- Advanced guides for Windows privacy, online protection and disaster recovery

Everything you need to keep your home network and smart devices safe and secure

100% INDEPENDENT

Papercut

Save a whopping 25% Off!

ALL Tech Manuals

with Papercut

Not only can you learn new skills and master your tech, but you can now SAVE 25% off all of our coding and consumer tech digital and print guidebooks!

Simply use the following exclusive code at checkout:

NYHF23CN

www.pclpublications.com

TRICKS & TIPS

Home Networking

Home Networking Tricks & Tips is the perfect digital publication for the user that wants to take their skill set to the next level. Do you want to enhance your user experience? Or wish to gain insider knowledge? Do you want to learn directly from experts in their field? Learn the numerous short cuts that the professionals use? Over the pages of this new advanced user guide you will learn everything you will need to know to become a more confident, better skilled and experienced owner. A user that will make the absolute most of their smart devices and ultimately home networking itself.

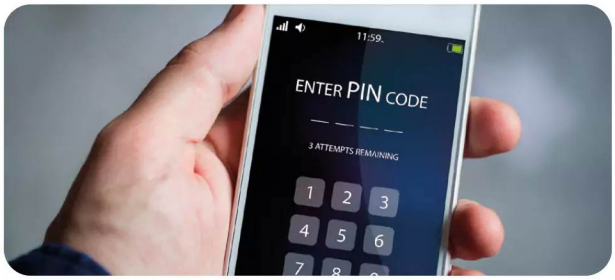
An achievement you can earn by simply enabling us to exclusively help and teach you the abilities we have gained over our decades of experience.

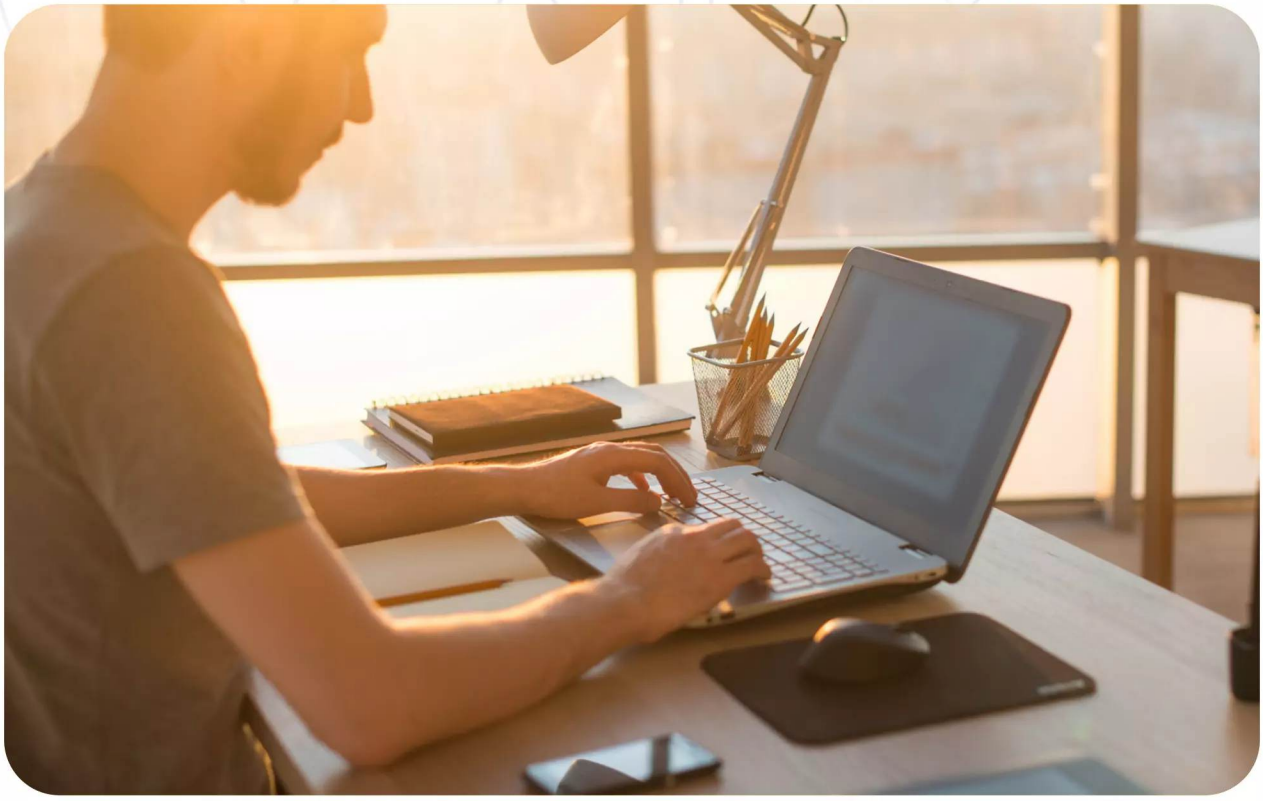
Over the page our journey continues, and we will be with you at every stage to advise, inform and ultimately inspire you to go further.

Contents

HOME NETWORKING

6 Online Protection & Disaster Recovery





32 Advanced Security Tips


Online Banki
Username
Password
Login
PREMIUM Credit
1234 56 78 9012 3
01/20

ONLINE PROTECTION & DISASTER RECOVERY

While you can successfully protect yourself and your own computer offline, as soon as you make a connection to the outside world, you're under the influence of many external factors. We'll 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, and when you're out and about with your Windows laptop and other devices.

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:

  1    <1 ms    <1 ms    <1 ms  broadband.bt.com [2a00:23c4:7591:7200:ae84:c9ff:feb6:f097]
  2     *        *        *     Request timed out.
  3     *        *       11 ms  2a00:2302::1100:100:36
  4    16 ms     8 ms     8 ms  2a00:2302::1100:100:37
  5    10 ms     9 ms     9 ms  2a00:2380:300c:b000::e
  6     8 ms     8 ms     8 ms  2a00:2000:2066::4a
  7     9 ms     9 ms     9 ms  ae-6.r04.londen05.uk.bb.gin.ntt.net [2001:728:0:5000::6b5]
  8     8 ms     8 ms     8 ms  ae-0.r24.londen12.uk.bb.gin.ntt.net [2001:728:0:2000::5d]
  9     9 ms     9 ms     9 ms  ae-1.r25.londen12.uk.bb.gin.ntt.net [2001:728:0:2000::152]
 10    11 ms    12 ms    11 ms  ae-2.r02.londen01.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

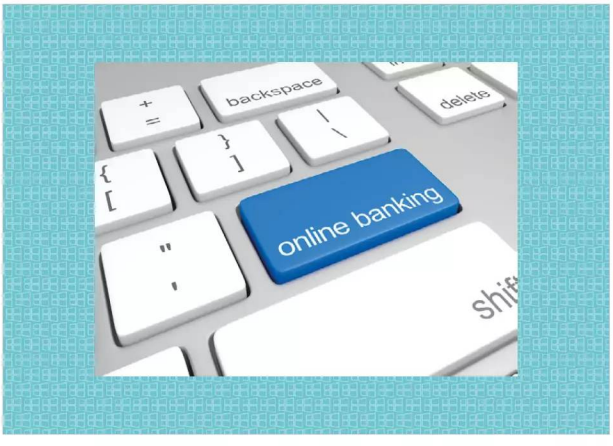
Despite the different and varied ways a hacker can gain access to your inbound and outbound data, there are means in which you can defend yourself. Here are ten tips to help you protect your data from being intercepted.

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.

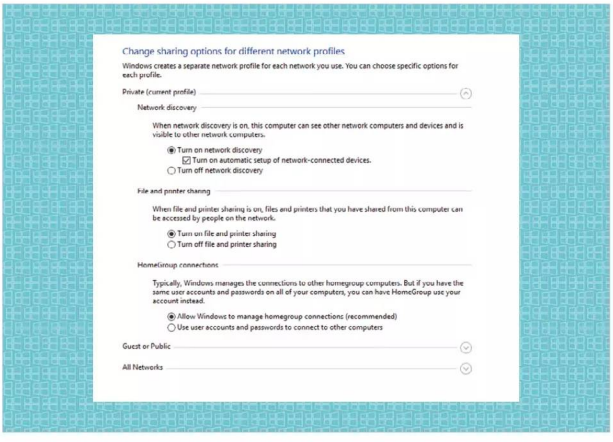
TIP 3 Always double-check a website for spelling errors, older logos or anything else that may raise an alarm. If your banking website looks even remotely different from when you last used it, try and avoid logging into it until you get to a more secure Internet location.

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.

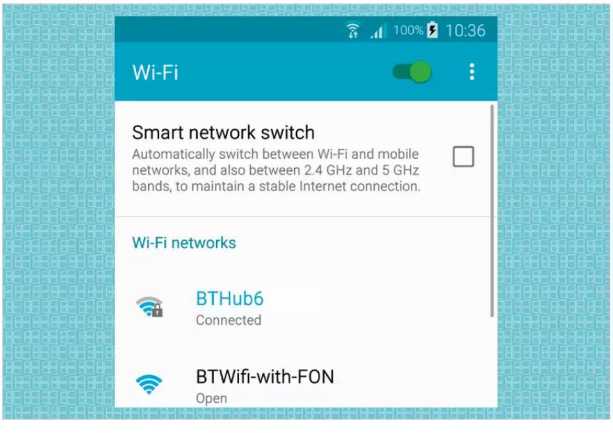


TIP 5 Always use HTTPS to access any website. This means that the information and data packets will be sent and received in an encrypted form and will make it exceedingly difficult for a hacker to decipher them. If possible, use an add-on such as HTTPS Everywhere for your browser of choice.

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 not 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

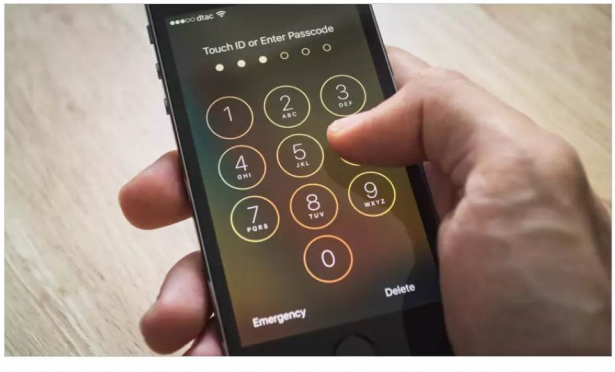
Mobile device hacking is on the rise. Most people now carry a phone or tablet around with them all the time, containing their emails, browser data, photos and enough personal information for someone to be interested.

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.

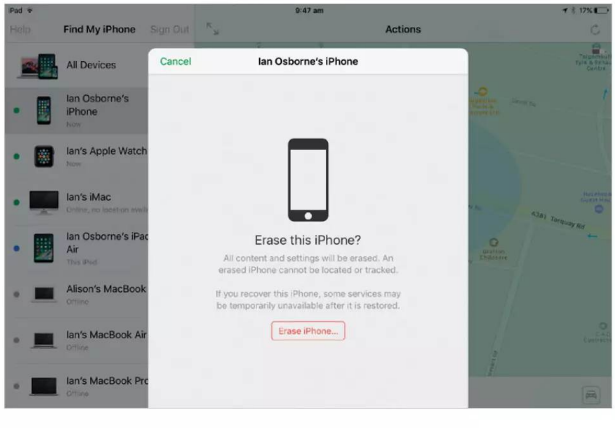
SECURITY LOCK

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.



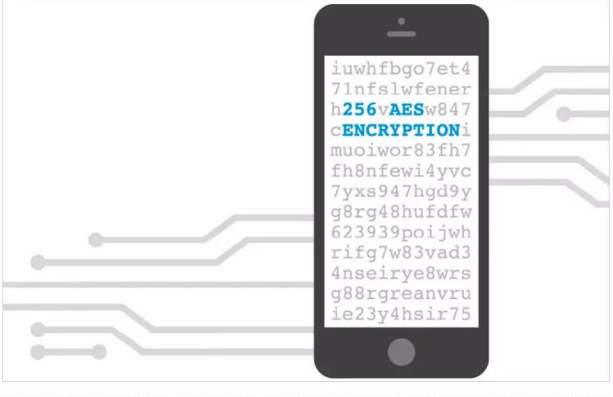
REMOTE WIPE

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.



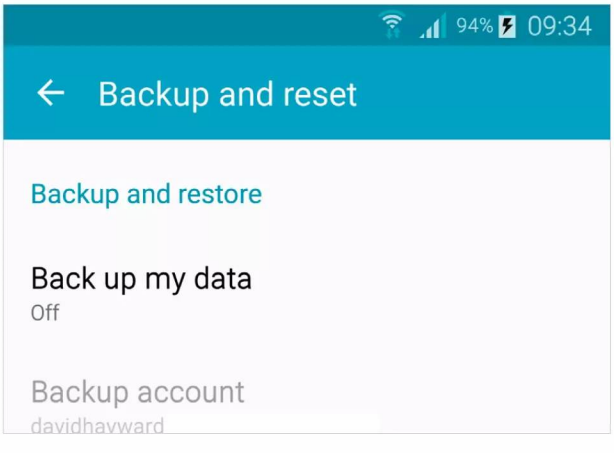
MOBILE ENCRYPTION

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.



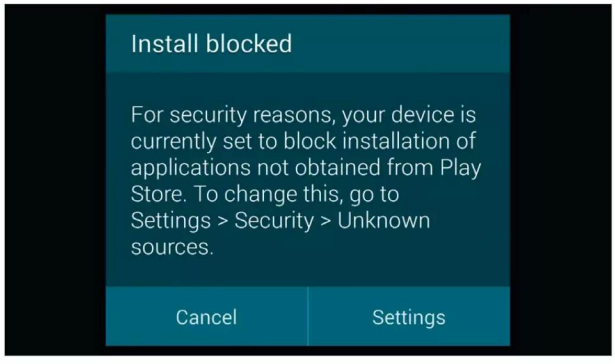
BACKUP DATA

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

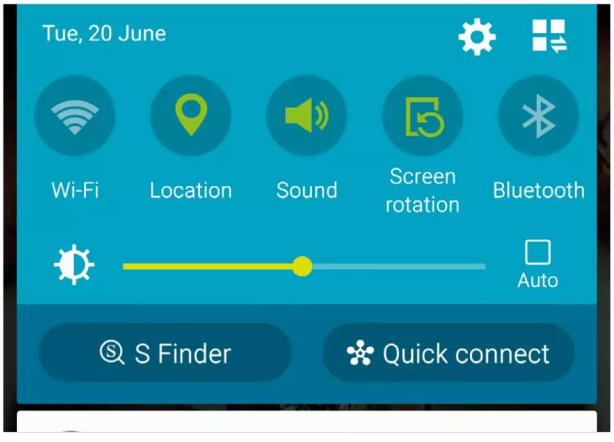
Keep your system as up to date as possible. It can be a pain having to frequently accept update and upgrade messages from your device, and waiting for the OS or the app to update itself, but more often than not an update will provide much needed security patches.

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

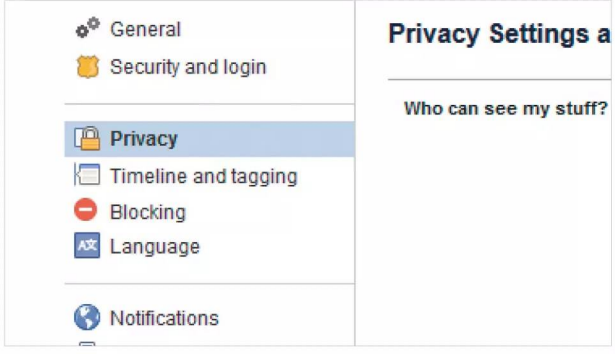
Facebook has become one of the best sources for cyber criminals to gain personal information on the Internet. Without realising it, a user is giving out reams of data and in most circumstances they're making it public.

Tips for Better Facebook Profiles

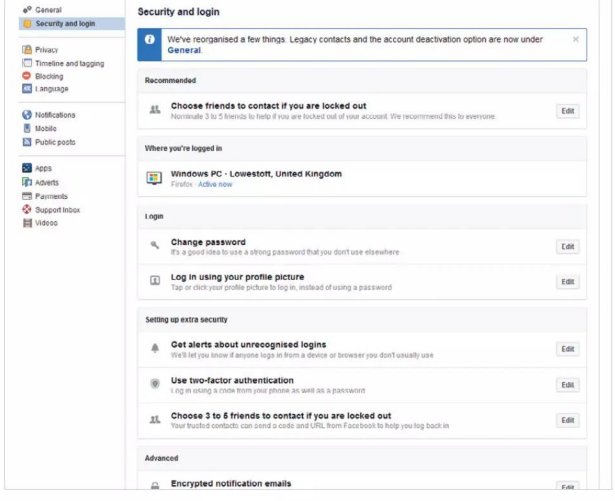
The dangers of social media aren't just for young people, many adults have been duped into befriending someone they don't know and exposing their personal information.

Facebook's policy forbids the use of fake names but it does allow nick 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.

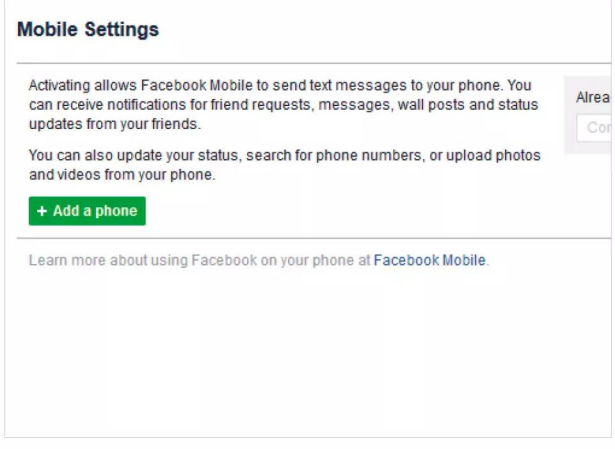
Go to Settings > Privacy, and make sure that the Who can see my stuff section is set for just friends, as opposed to friends of friends or public. This will effectively hide your Timeline contents from others and only your confirmed friends will be able to see any updates.



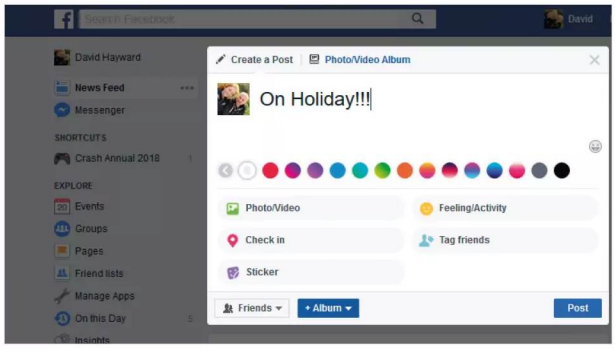
Set up two-factor authentication, alerts about unrecognised logins and make sure that emails from Facebook are encrypted. These can all be found in the Settings > Security and Login section.



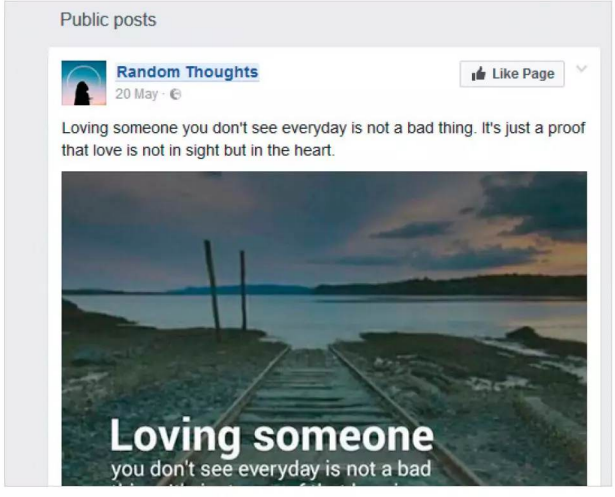
Never post any contact information on your profile. We often automatically start filling in the phone number field on a site but take a moment to consider what the ramifications could be should your number be made aware outside your circle of friends. That also includes house address too.



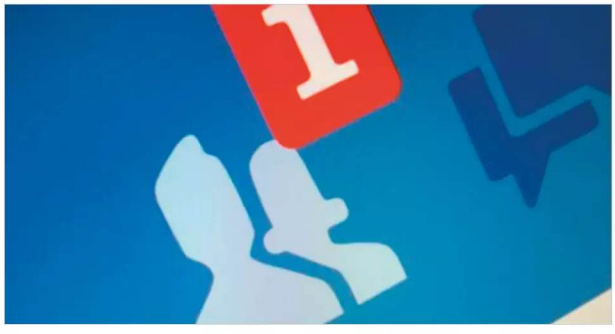
Tempting as it may be, try to avoid posting your location. Whether you're at home alone, or you're on holiday, should that information be made available then a criminal will know that your house is empty or worse, that you're alone in it.



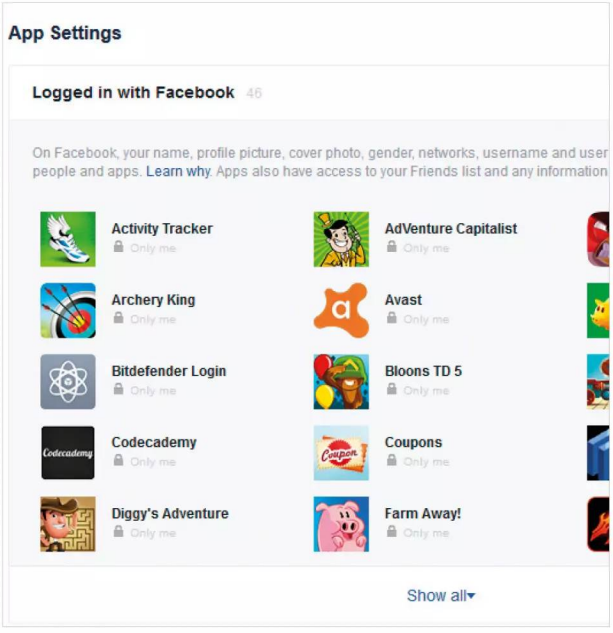
Try and avoid sharing random thoughts of the day, inspirational quotes, fake news or other such items that appear on your Timeline from others. Often these instances are created to farm for shares and likes and as such can often be traced back to individuals who are simply looking for active Facebook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



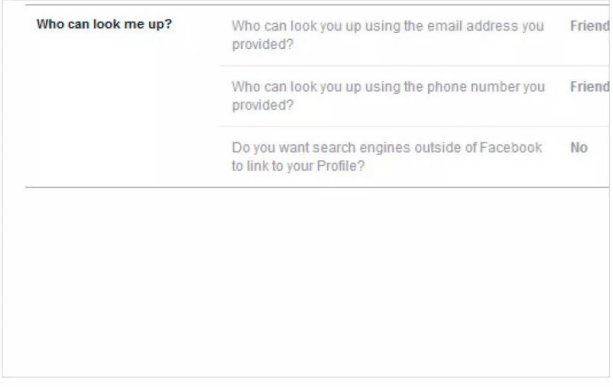
Try not to accept every friend request you get. Take a moment to check the person out and if necessary message them to find out who they are and how they know you. If their comment is something like 'we met at the bar last month' then it's best to ignore the request, as they could be fishing for information.



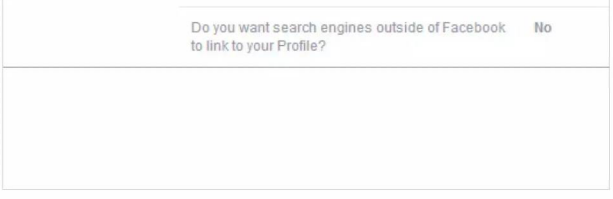
Not all apps you install on your phone or tablet are good. Take a moment to read what an app will try to access when it's installed. Often a rogue app will attempt to access your Facebook account to farm for your and your friend's information.



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.



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.



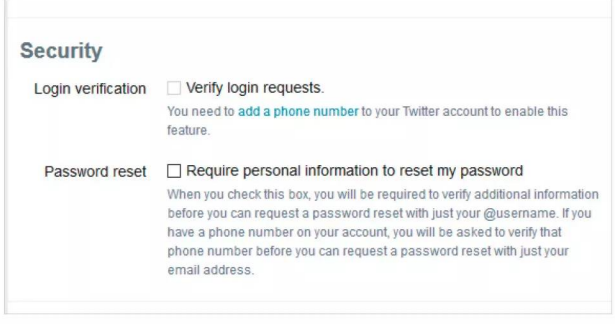
How to Secure Yourself on Twitter

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.

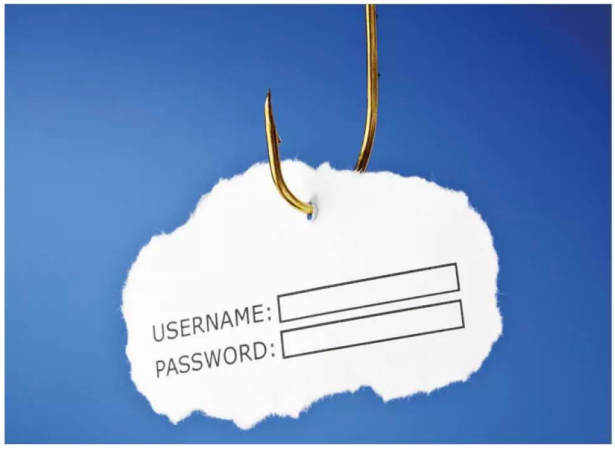
Securing the Twitterverse

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.



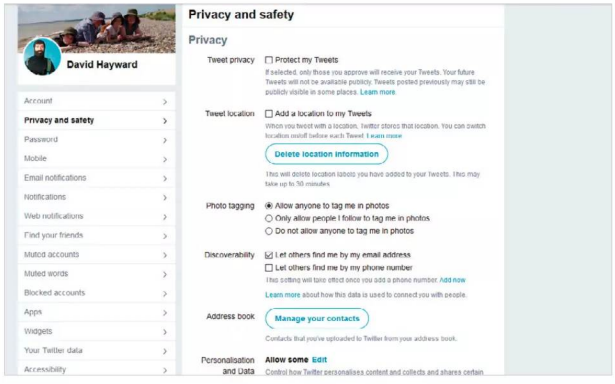
Just like most other social media platforms, phishing scams are rife on Twitter. Be wary of anyone sending you Tweets claiming to be someone you know, offering a too-good-to-be-true job or even informing you that your account is compromised. It's likely a phishing scam, so delete and report the instance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

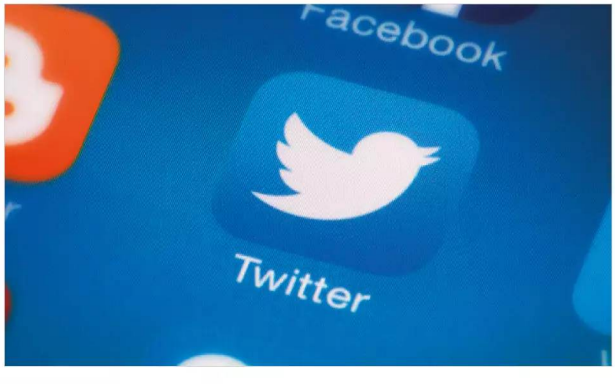
There are many accounts on Twitter that simply aren't real. These bots, as they're known, can be programmed to post daily amusing, inspiring and socially acceptable Tweets. On the flip side, other bots are designed to Tweet suspicious links to virus-infested websites. In short, unless you trust the account,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

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.

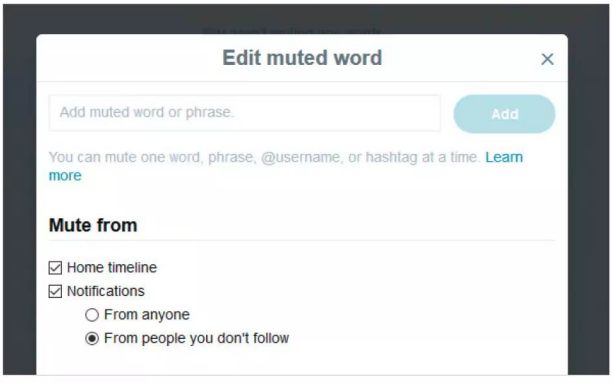


Direct messaging in Twitter is both advantageous and dangerous at the same time. Whilst great for communicating directly with another user, it's also used by others to lure in victims or send links to malicious websites. It's best to ignore most messages unless you know who they're from.

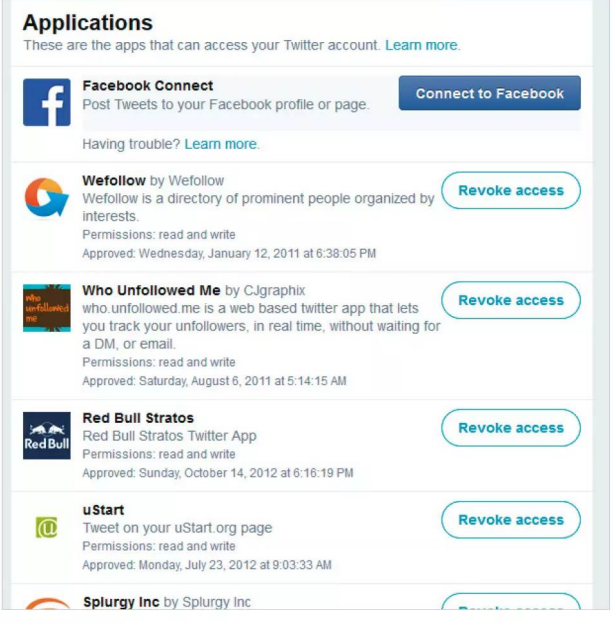
If you use your Twitter account to login into any third-party apps or games, then you may need to consider setting up a secondary Twitter account. Whilst convenient, some apps can be hijacked to collect account details, leaking them to hackers.



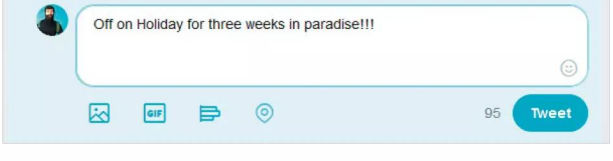
Word Muting is an excellent feature within Twitter's account settings. With it you're able to mute any words you don't want to see in your notifications or timeline. There are often Tweets you'd like to avoid even seeing in your timeline, so muting them is an ideal solution to help keep your account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



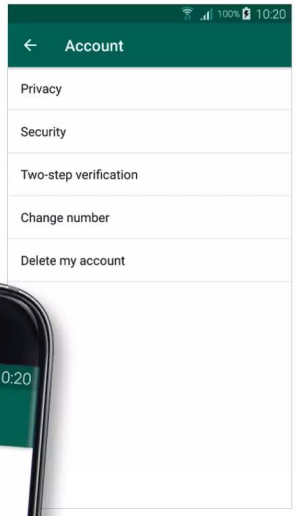
How to Secure Yourself on WhatsApp

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.

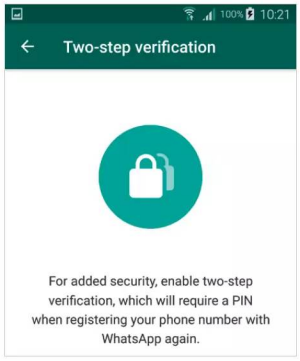
WhatsApp Security Tips

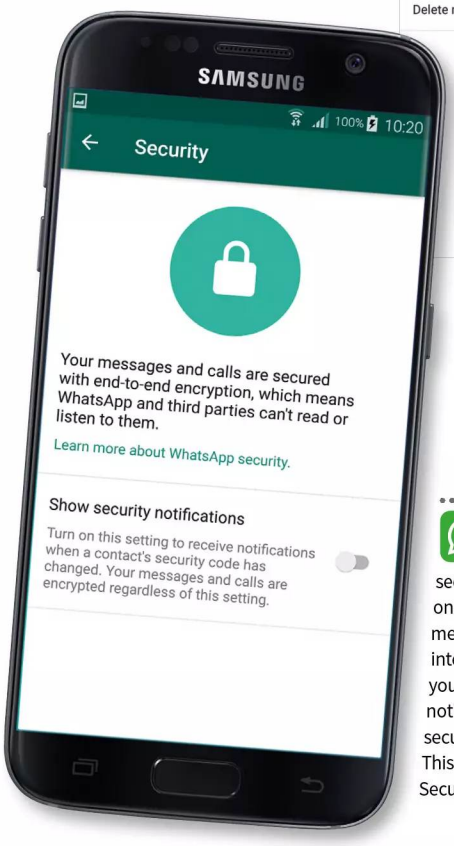
With this popularity comes a darker side to messaging. Accounts of terrorists using WhatsApp, along with hackers, scammers and all manner of nefarious individuals and groups are ever in the popular media.

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.



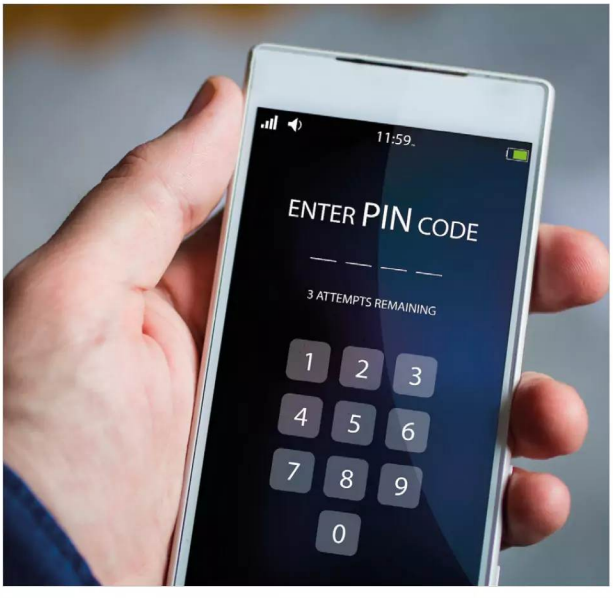
For added security you can opt for two-step authentication, which will require a PIN when registering your phone number with WhatsApp. This is an absolute must for those who use the app regularly.





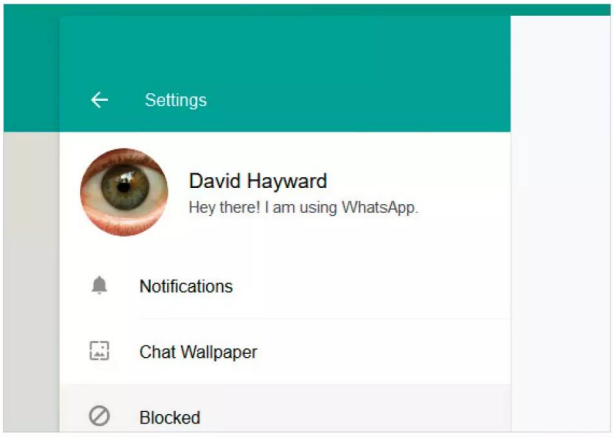
Thankfully, WhatsApp already encrypts and secures messages sent from one device to another. This means that your data can't be intercepted and read. However, you can opt to view security notifications if a contact's security setting has been altered. This is in the Settings > Account > Security menu.

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.

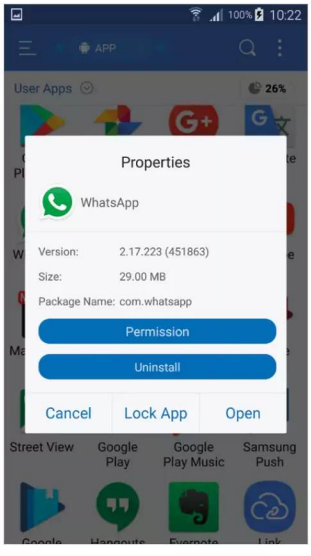


Generally you're not able to add users to your chat list if you don't already have them in your contacts list. However, clever phishing scams can have a victim add a contact, who can then message them using WhatsApp; as with all social media platforms, be wary of phishing attacks.

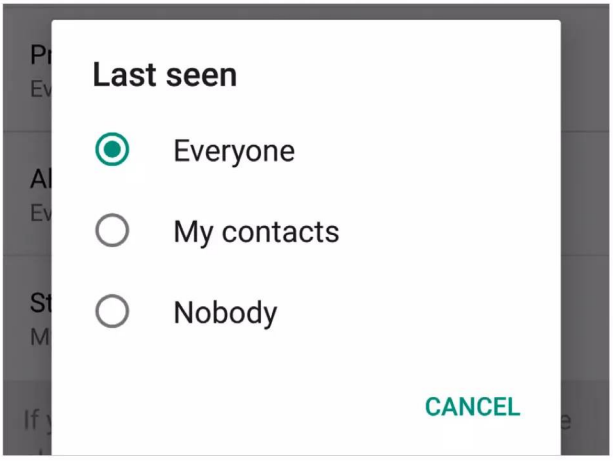
You can block users via the WhatsApp Web feature. Log into WhatsApp Web, and click on the three horizontal dots by your profile picture. Then click Settings and from there the Blocked option. You can select contacts to block from WhatsApp.



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.

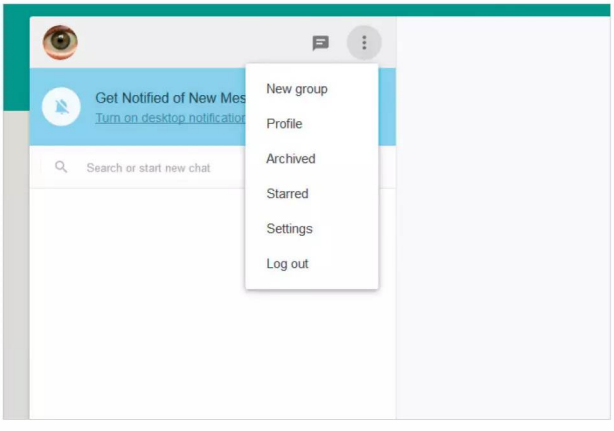


If you don't want WhatsApp contacts to see where you've been, you need to disable the Last Seen option within the Privacy settings. This will prevent other users from 'seeing' your movements. Should a malicious contact be added, they will never know where you are or have been.



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

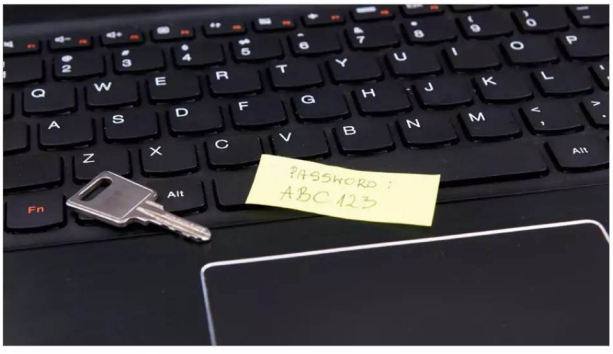
To help you create the perfect password, and secure it further, here are ten tips for happier password management. There's always password pitfalls but stick to these general tips and you should be okay.

OBVIOUS DATES

Never use your date of birth, partner's date of birth, children's date of birth, pet's names, family names or even the town where you grew up in. This is all information that can easily be collected from social media 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 not too difficult for someone to visit your computer whilst you're on a coffee break and read the note.



SAME PASSWORDS

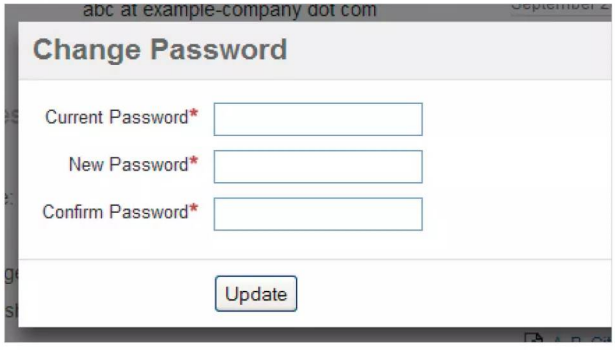
Never use the same password for multiple sites. It's tempting and easy to have a single password for everything but should that password ever become compromised you will lose access to every site you visit, including any banking sites.

COMMON PASSWORDS

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"o% 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

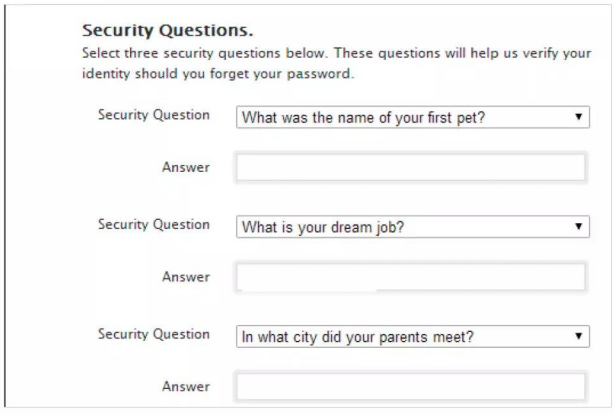
Try to avoid logging into certain sites when you're using public Wi-Fi. We've already covered how data on a public, free Wi-Fi access point can be intercepted. Your passwords, therefore, can be intercepted and viewed in plain text by a hacker.

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.

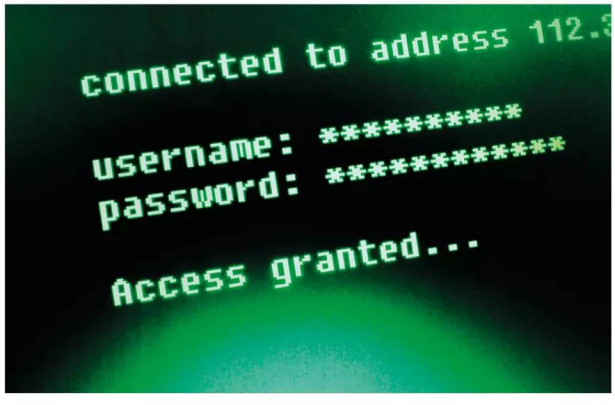
SECURITY QUESTIONS

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

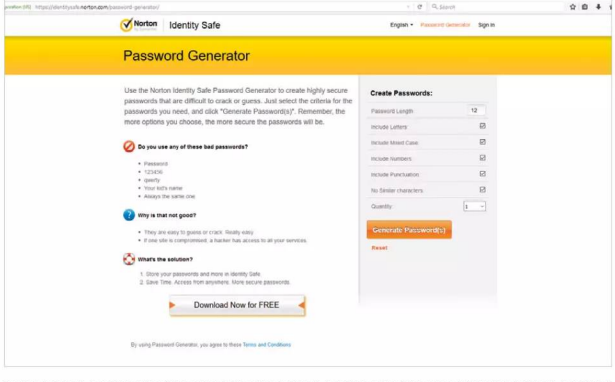
We've looked at some tips on what not to include when coming up with a strong password. However, it's not always as straight forward as that. Whilst some can come up with an elaborate and incredibly strong password, others struggle. Thankfully, there's help on offer.

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.

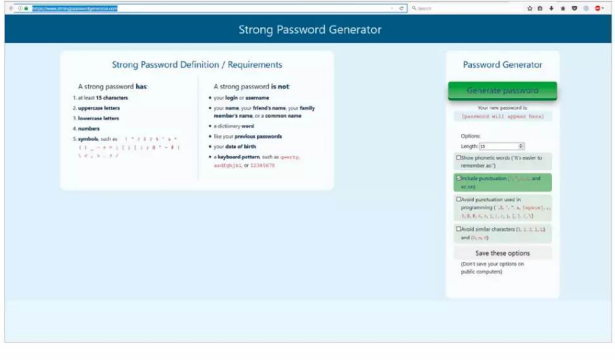
NORTON IDENTITY SAFE PASSWORD GENERATOR

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/**.



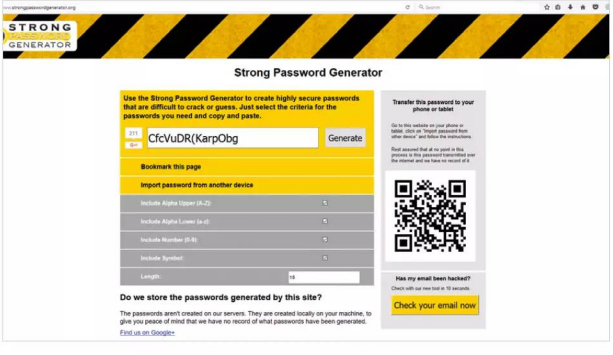
STRONG PASSWORD GENERATOR

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/**.



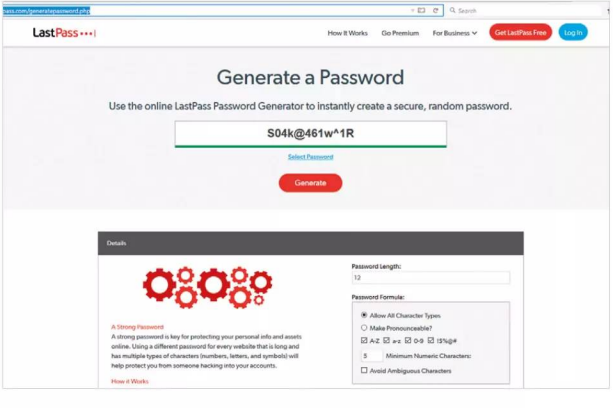
WIGHT HAT PASSWORD GENERATOR

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.



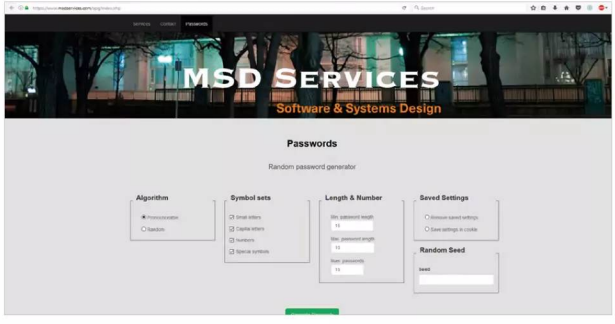
LASTPASS

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.



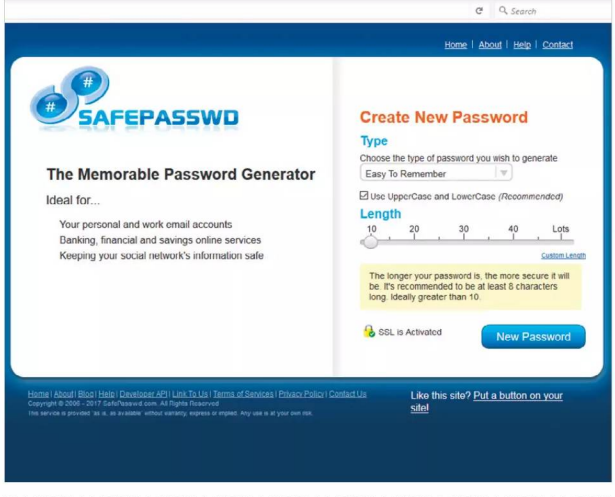
MSD SERVICES

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.



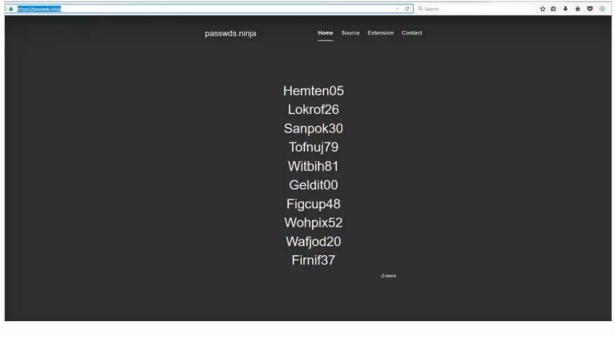
SAFEPASSWD

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/**.



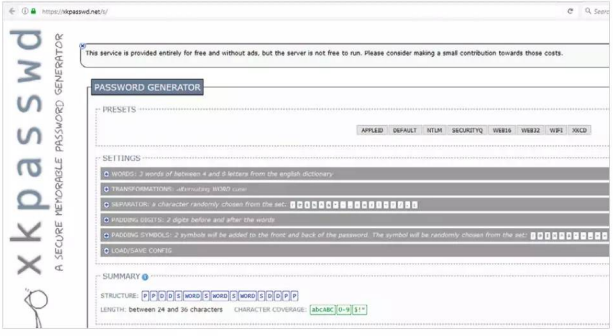
PASSEDS.NINJA

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.

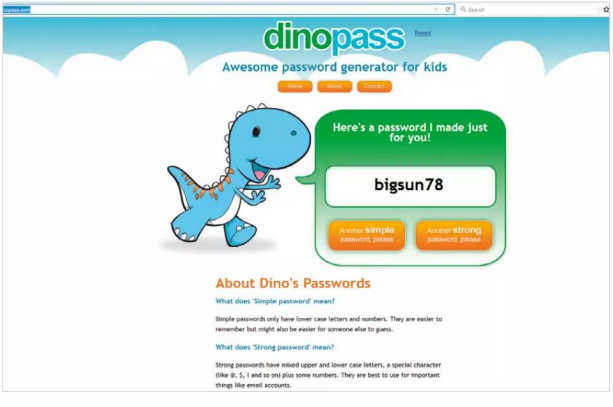


LITTLELITE PASSWORD GENERATOR

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 synching, 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 synching 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.

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.**

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.

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.

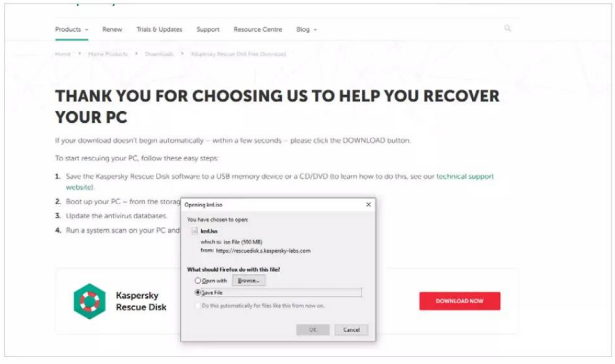
How to Remove a Virus or Malware from a Windows PC

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.

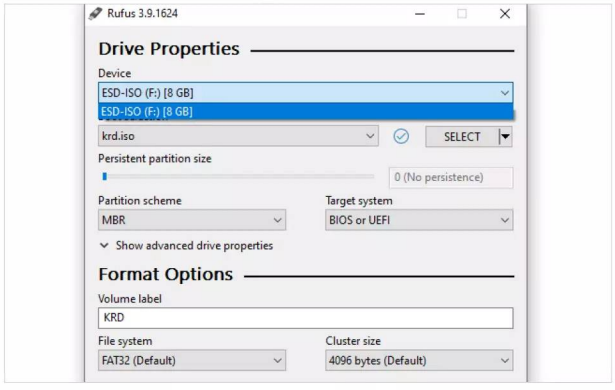
Malware Busters

For this tutorial we'll use a pre-configured rescue disk from Kaspersky. We'll 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.

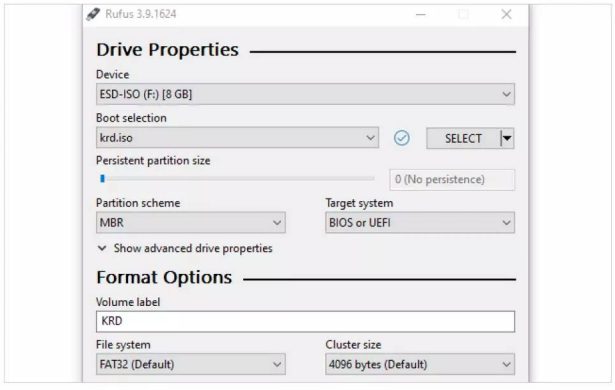
STEP 1 Make sure you have a blank CD or a USB stick that's at least 1GB in size. The Kaspersky Rescue Disk is downloaded as an ISO (which is an image file containing all the disk information), and can be downloaded from **https://www.kaspersky.com.au/downloads/thank-you/free-rescue-disk.**



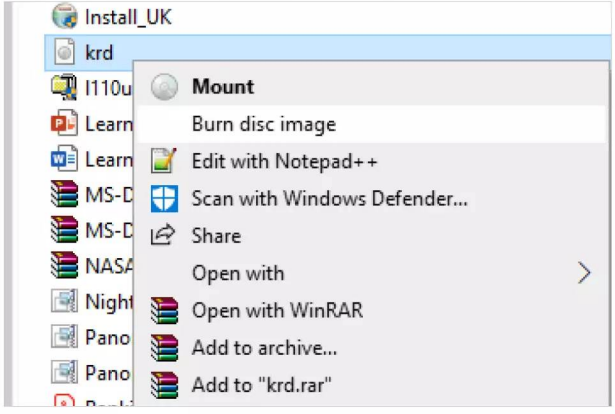
STEP 2 To transfer the ISO to USB download Rufus; which is an executable that doesn't require any installation, and can be downloaded from: https://rufus.ie/. Insert your USB stick and double-click Rufus. Check that the Device label is pointing to your inserted USB stick, if not then you may need to close Rufus, remove the USB, then re-insert the USB and re-start Rufus. The remaining options can be left as their defaults.



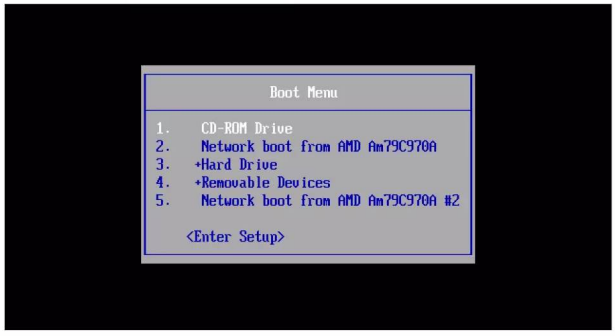
STEP 3 Click the Select option, and using Windows Explorer, locate the downloaded Kaspersky Rescue ISO – it'll be called krd.iso. Click the Start button to select the image and continue with the process. This will copy the contents of the ISO to the USB while also making the USB a bootable device.



STEP 4 If you're using a CD, start by inserting the CD into the drive. Locate the downloaded Kaspersky 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.



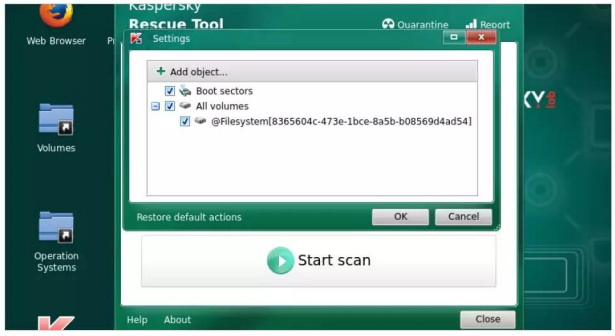
STEP 5 You'll now need to allow your PC to boot up into the Kaspersky Rescue CD environment. Power up your PC and open the Boot Option Menu. This could be accessed by pressing F12 (depending on the make and manufacturer of your PC motherboard). With the boot options available, select either the CD or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



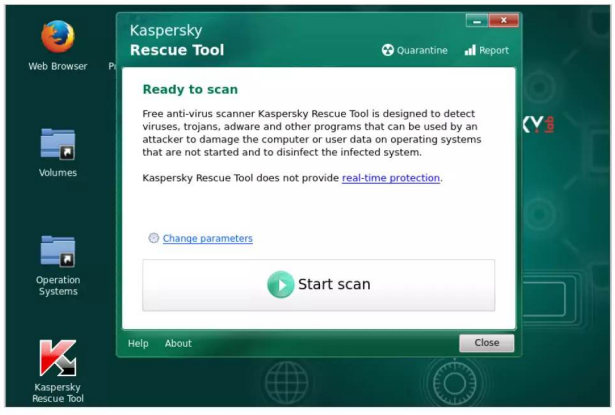
STEP 6 The PC will now boot into the Kaspersky Rescue Disc environment. This is a custom Linux operating system with all the necessary security tools pre-installed. First, you'll need to choose which language to load the environment in. Use the arrow keys, and press Enter for your language choice. After that, choose the Graphic Mode.

STEP 7 Begin by accepting the license agreement. After that, the rescue disc will check its status and open a window asking for you to start scanning the system. However, it's best to check you've got access to the Internet in order for it to update first. Close down the Rescue Tool window, and click on the Network box in the bottom-right. Connect to Wi-Fi, or Wired as required.

STEP 8 Once connected, relaunch the Kaspersky Rescue Tool from the desktop icon, agree to the license once more. Before you begin, click on the Change Parameters link in the Kaspersky Rescue Tool window. This will enable you to choose which drives the tool can scan for infections and malware. Tick all the drives in your system.



STEP 9 When you're ready to continue, click on the Start Scan button in the Kaspersky Rescue Tool window. This will begin the process of scanning all the drives selected in the previous step. Be aware, that, depending on the size of your drives and the amount of data on them, this could take quite some time.



STEP 10 While the scan is working, you'll see the object that the tool is currently processing. You'll also get a brief run-down of any threats currently found, time taken, and number of files scanned. Once complete, you can view a report by clicking on Details. Hopefully, you're malware free, and you can remove the USB/disc and reboot the system.

ADVANCED SECURITY TIPS

If you want to improve your Windows security further, then this section will look at more advanced ways and means in which you can achieve that goal. We cover firewalls, sandboxing and virtual environments, and how to tell which programs are communicating beyond your home network.

Our easy to follow tutorials will help you create a reliable backup of Windows and all your data, so should something unfortunate happen, you'll be able to restore your files with confidence.

Windows Privacy Settings

Windows's new updates and special edition 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.

Windows is said to be the last true Windows desktop release, with the Redmond company

> ***Going Private***

now opting for a rolling release cycle, that will add or remove features over time through regular updates.

There are many advantages to this particular setup. A Windows user will always be up to date with regards to security, options and support. Any new hardware that's released will be added to the vast driver database that Windows already uses and it will operate at its maximum potential. Microsoft can gradually roll out features that would require a brand new operating system, thus maximising the capabilities of the OS. Of course, the company can charge for certain additional features that would ordinarily be a part of the OS, such as a media centre for example.

However, profit margins aside, it's the rolling security and updates that the user will benefit greatly from. As Microsoft evolves Windows, user and developer feedback can help improve the way the OS protects its user base. A prime example is the new privacy settings available post-Fall Creators Update, which was gradually rolled out to Windows PCs around late October 2017. The privacy settings and options that are now on offer are a radical improvement over the previous, rather bleak, features that came with the original Windows setup. Now, the user has greater control over what the OS can and cannot do to affect an individual's privacy.

Providing you've applied the Fall Creators Update, you can view the current privacy options by clicking the Windows Start button and typing privacy into the search box. Click on the Privacy Settings option, with a padlock icon, and the core privacy options window will open. There are, at the time of writing, nineteen different options available to browse through. Each option, when clicked, will display a subset of available options that can then be enabled or disabled and turned on or off, depending on your preference.

For example the first option, General, offers the user a choice of opting for advertising via apps, allowing websites to provide locally relevant content based on the user's language list and allowing Windows to track how an app is launched to improve search results. Whilst that in itself doesn't sound too much like your privacy is being infiltrated, there are those who don't want the installed apps and the OS having too much knowledge of where they are and what to advertise. Like most privacy options, it's a personal preference as to what you're happy sharing with the system and its connected technologies. Whilst opting to turn every privacy setting on will inevitably open your use of Windows up to whoever or whatever is readily receiving the information, likewise turning everything off will effectively hide you (to some degree); but at the cost of possible loss of available features. There's a fine balance needed to get the best from your privacy and still enjoying Windows's many features.

There are some interesting additions to the Fall Creators Update privacy settings, which are certainly worth looking over, if you want a best of both worlds approach to privacy and features.

Location – The Location option will allow Windows and its apps to use your current location to specialise any content. It's innocent enough but for added privacy it's worth considering turning it off.

Camera – This is an excellent addition that will define which installed apps have access to the computer's webcam. You can turn off app access to the camera globally or browse through the apps to decide which has access, or not.

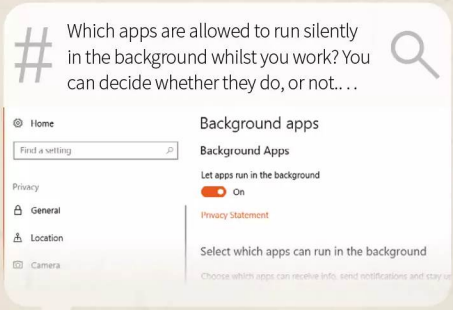
Microphone – The same applies for the computer's microphone; which apps can access it or not, and whether you want to globally turn it off.

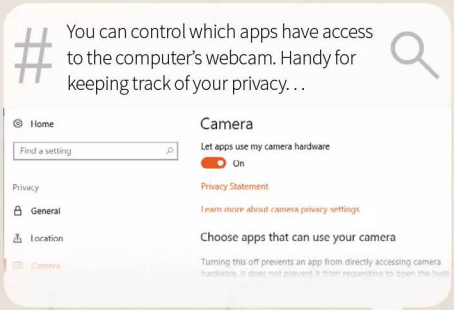
Contacts – The Contacts section details which apps can have access to your current Windows account contacts. Disabling this globally may have a severe impact on how some apps, such as Skype and email work.

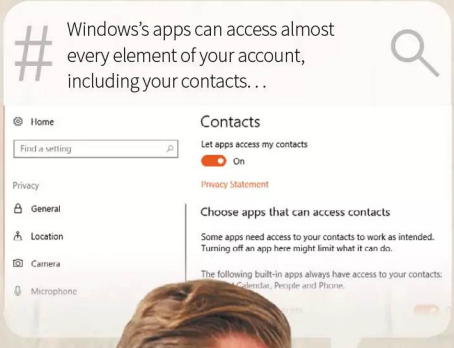
Radios – This option will define which apps can control hardware such as the computer's Bluetooth device, Wi-Fi or any other kind of wireless receiver. Obviously, some apps will require access to share information or allow access to shared areas.

Background Apps – Windows's background task handling is far better than in previous versions of the operating system. Memory is released as apps drop into the background, as is processor allocation. However, you can further define which apps will be allowed to run in the background with this option.

Taking time to go through each of the available options is something every Windows user should do. This way you become familiar with how the OS shares your account data and what exactly has access to your Windows computer and its hardware.







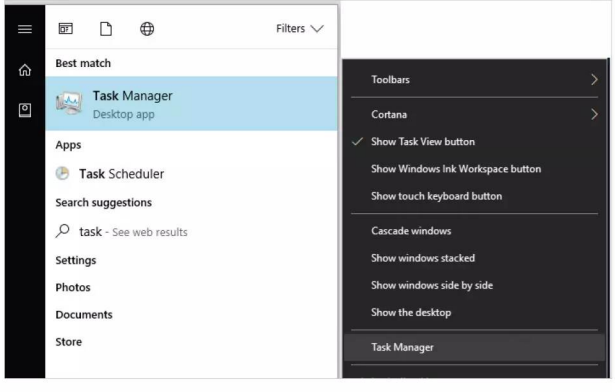
How to Check which Apps are Sending Information

Most Windows apps and programs have some element of code that will attempt to communicate with an external source. That communication could be to check for the latest version, or patches and updates, or it could be malicious software sending personal data.

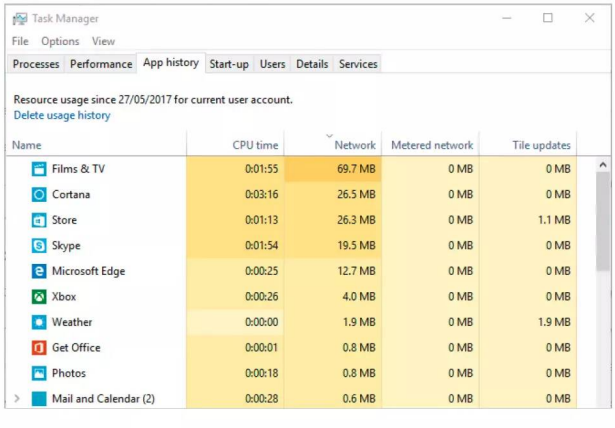
Look Who's Talking

There are a number of ways in which you're able to view which programs and apps are sending data to Internet and external sources. Some methods are better than others, so it's worth trying them all to see which works best for you.

STEP 1 The first port of call to help monitor what apps are accessing the Internet is Task Manager. Click the Windows Start button and type task, then click the Task Manager result in the search box. You can also right-click the taskbar and select Task Manager from the available option in the menu.



STEP 2 With Task Manager displayed, click the More Details arrow (if it's available). This will expand the Task Manager options. From here, click the App History tab and then the Network column so that there's a downward pointing arrow above it. This indicates network use in a descending order of amount of data sent.

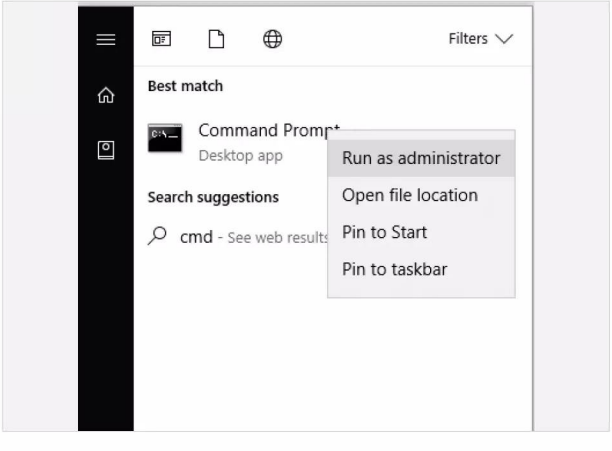


Name	CPU time	Network	Metered network	Tile updates
Films & TV	0:01:55	69.7 MB	0 MB	0 MB
Cortana	0:03:16	26.5 MB	0 MB	0 MB
Store	0:01:13	26.3 MB	0 MB	1.1 MB
Skype	0:01:54	19.5 MB	0 MB	0 MB
Microsoft Edge	0:00:25	12.7 MB	0 MB	0 MB
Xbox	0:00:26	4.0 MB	0 MB	0 MB
Weather	0:00:00	1.9 MB	0 MB	1.9 MB
Get Office	0:00:01	0.8 MB	0 MB	0 MB
Photos	0:00:18	0.8 MB	0 MB	0 MB
Mail and Calendar (2)	0:00:28	0.6 MB	0 MB	0 MB

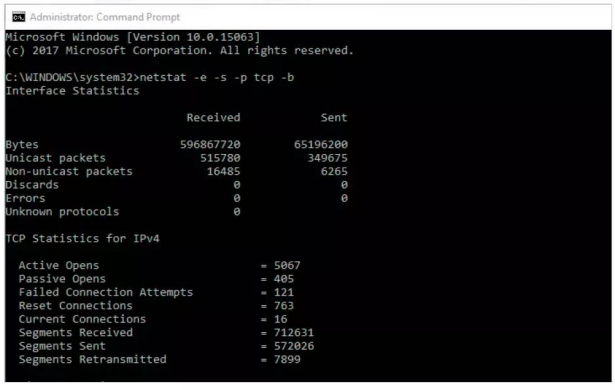
STEP 3 This is a reasonably accurate way of viewing which installed programs have been accessing the outside world. The amount of data being sent to and from your PC can be quite illuminating, and surprising, as you may never even realise you have a particular app installed never mind that it's communicating with an external source.

Films & TV	0:01:55	69.7 MB	0 MB	0 MB
Cortana	0:03:16	26.5 MB	0 MB	0 MB
Store	0:01:13	26.3 MB	0 MB	1.1 MB
Skype	0:01:54	19.5 MB	0 MB	0 MB
Microsoft Edge	0:00:25	12.7 MB	0 MB	0 MB
Xbox	0:00:26	4.0 MB	0 MB	0 MB
Weather	0:00:00	1.9 MB	0 MB	1.9 MB
Get Office	0:00:01	0.8 MB	0 MB	0 MB
Photos	0:00:18	0.8 MB	0 MB	0 MB
Mail and Calendar (2)	0:00:28	0.6 MB	0 MB	0 MB
Sport	0:00:01	0.5 MB	0 MB	0.5 MB
OneNote	0:00:01	0.1 MB	0 MB	0 MB
Twitter	0:00:01	0.1 MB	0 MB	0 MB

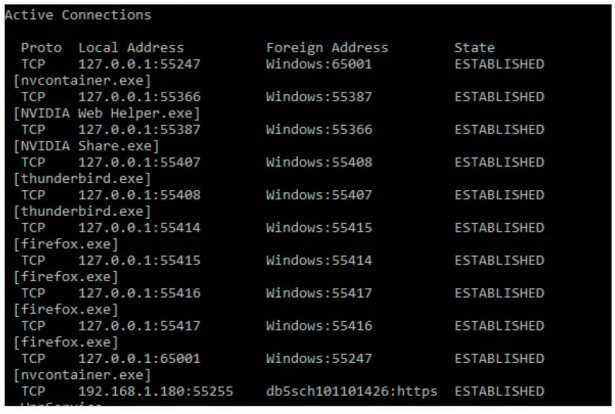
STEP 4 Another excellent method is by using the Netstat command. Click on the Windows Start button and enter **cmd**, then right-click the Command Prompt option and choose Run as Administrator from the menu. When the message to authenticate the action pops up, click on Yes.



STEP 5 With the command prompt open enter the following: **netstat -e -s -p tcp -b**. The information populates the command prompt box quickly, so you need to scroll back up to the top to see it in its entirety.

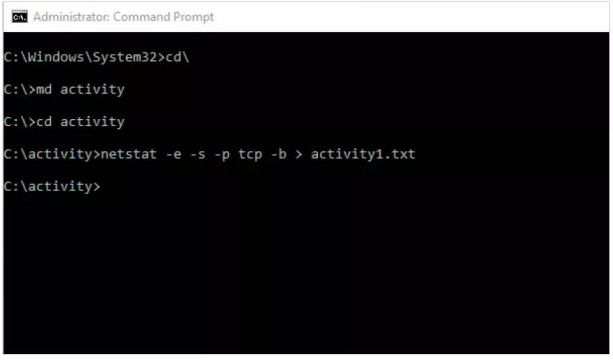


STEP 6 What you're looking at here is a list of programs, from the column to the far left, with the IP address of its source and the destination address in the middle column; with a third column detailing if the connection is established or not. It can be confusing to view at first but after a moment or two it should begin to make sense.

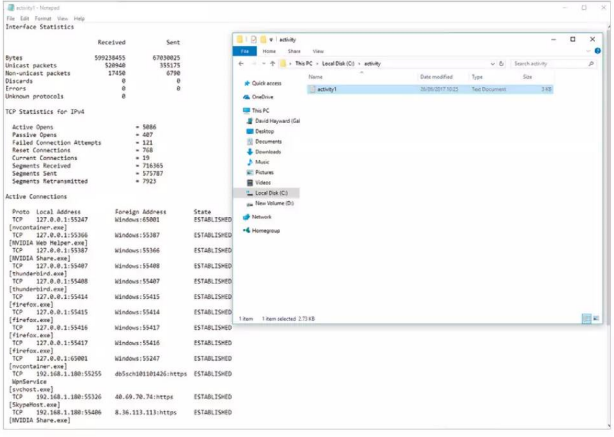


STEP 7 If you want to create a friendlier way of viewing Netstat active connection data, you can pipe the contents to a text file. For example, in the command prompt enter **cd** to take you to the root of the C: drive. Then create a new folder to store the text file with **md activity**, and enter it with **cd activity**.

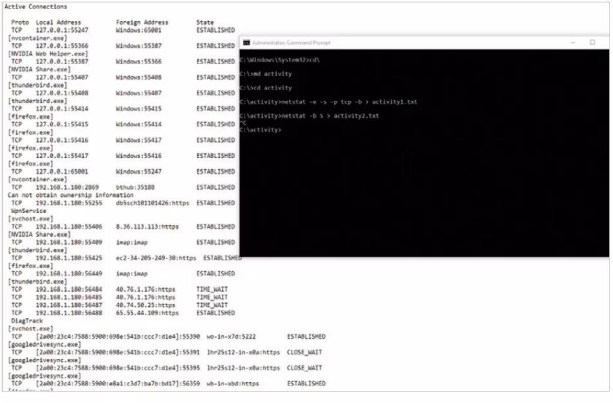
STEP 8 In the activity folder, enter the following: **netstat -e -s -p tcp -b > activity1.txt**. This is the same command as before but this time the output is being sent to a text file, named activity1.txt, rather than outputting to the command prompt window.



STEP 9 Using Windows Explorer, locate the C:\activity folder you created and within the activity1.txt file. Double-click the **activity1.txt** file and it opens in Notepad where you're able to view it without the often difficult to read command prompt window.



STEP 10 If you want to simplify the information and the process, enter: **netstat -b 5 > activity2.txt** into the command prompt within the activity folder on the C: drive. This will record the information and only write the data once you've pressed **Ctrl+C**, which stops the process. Use this for around two minutes to get a record of what's going on.



What is a Firewall?

The data packets that come and go between your PC and the outside world can be defined by a set of rules. These rules state whether a packet has access to the system in the first place, then whether or not it can gain access to its destination program. Collectively, these rules make up a Firewall.

Great Walls of Fire

The term firewall comes from fire prevention, where a physical wall is constructed in order to halt the spread of a fire. In digital terms, the physical wall stops malware and other threats from spreading into the system.

Some form of digital protection against unwanted entry into a system has existed for many years but the more recent software side of a firewall, one that we're reasonably familiar with, has only been around since the '80s.

Prior to the modern firewall, system administrators blocked unwanted access through various stages of hardware layers. Long lists of allowed computer addresses were painstakingly entered into mainframes and routers, where programmable chips filtered the white list and simply stopped all access to addresses that weren't on the list; think of a nightclub bouncer, if your name's not on the list you're not getting in.

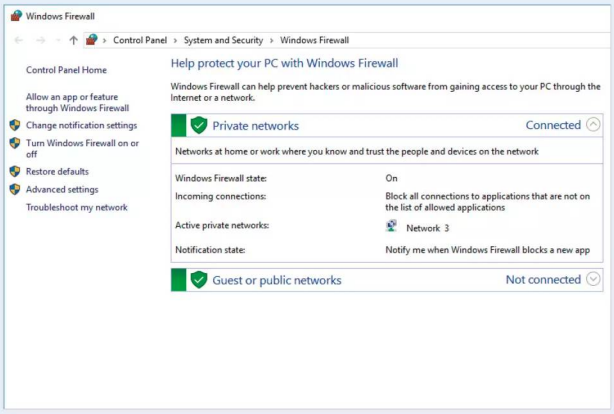
In its simplest guise, a firewall will look to a defined set of rules then apply those rules to any data packets that pass through it. For example, if you've created a rule whereby all Telnet traffic is blocked, any packet that's trying to reach port 23, the port that Telnet applications listen on for data, will be blocked. While suitably effective this low-level packet filtering does have its Achilles heel, in that it treats each packet as an independent piece of data: not knowing whether it's a part of an already established stream of data. This can be targeted by hackers who want access to a system with a firewall in place. The clever hacker is able to spoof a packet and thus tricking the firewall into letting it pass. It takes some time, and it's a bit hit and miss, but most hackers have plenty of patience when it comes to getting into a network. Therefore a much needed higher degree of firewall monitoring is called for.

Stateful Inspection firewalls were introduced in the mid '90s and enabled a firewall to log all the connection that passed through it determining what was the start of a new packet stream, part of an existing packet stream or something random. This allows a firewall to allow or drop any access based on a data packet's history. In terms of effectiveness, this makes the firewall more efficient and faster at dealing with connection requests as it doesn't need to continually analyse each packet as an individual but rather as a whole stream. For added layers of protection, if a packet doesn't match any of the connection histories, then it can be evaluated and filtered through the various rules to determine its legitimacy.

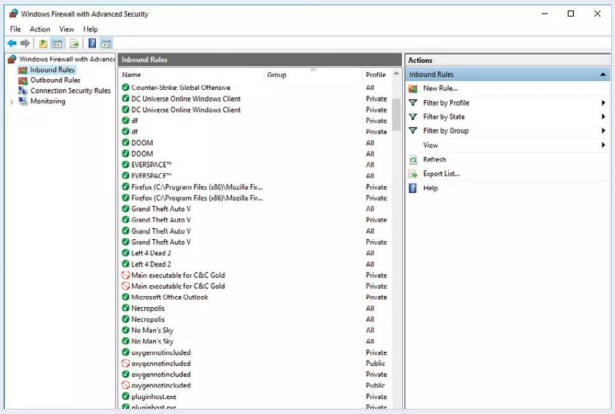
A further layer of protection was included into the basic firewall early in the 2000s. Application-layer analysis enabled firewalls to inspect packets that were targeting individual applications within the operating system. Each program or application installed in the system will use a set of protocols to communicate with the outside world. When an application is installed, on a Windows system for example, the installation mechanism will automatically add an instance of it to the Windows firewall. This means that it is able to send and receive information successfully through the Windows firewall without any of it being blocked. By blocking an application's access to the outside world, the user could miss out on regular updates, fixes, patches and so on. One of the key benefits to an application-layer firewall is that it's excellent at blocking specific content, such as known malware and viruses or dangerous websites. It's also capable of determining when a particular protocol is being misused by a rogue application.

Where the firewall proceeds from this point is unclear. However many experts agree that although we'll always need a firewall, the modern systems, networks and devices have so many potential access points that it's fast becoming less efficient to run the standard firewall model. In effect, the modern firewall, regardless of how complex and efficient it has become over the years, is quick becoming a bottle-neck for the operating system. What some experts are theorising is that at some point in the future, the need for a single, overall firewall will be outdated and that the next-generation operating systems will require each program and application that can be installed to act as its own firewall. Whether this will come about is pure fantasy at the moment but at the speed digital technologies grow and evolve there's a good chance of finding out soon enough.

> *Hardware firewalls are an early example of network security*



"The built-in Windows firewall is certainly good enough for most users' needs. It's fast, effective and can be easily configured."



"When each program, application, game and so on is installed, it is entered into the Windows firewall so it can communicate with the outside world."

"There are countless freely available third-party firewall clients. Some are very good, others not so much."

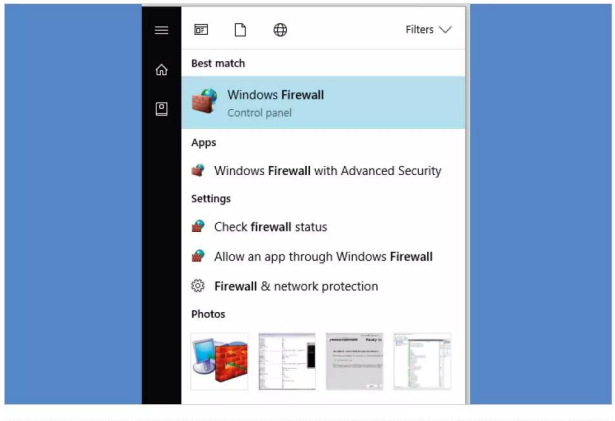
Improving the Windows Firewall

The built-in Windows firewall is a surprisingly good security application. Whilst it may not be as efficient as something offered by one of the third-party security suites, it's certainly more than adequate for the average user.

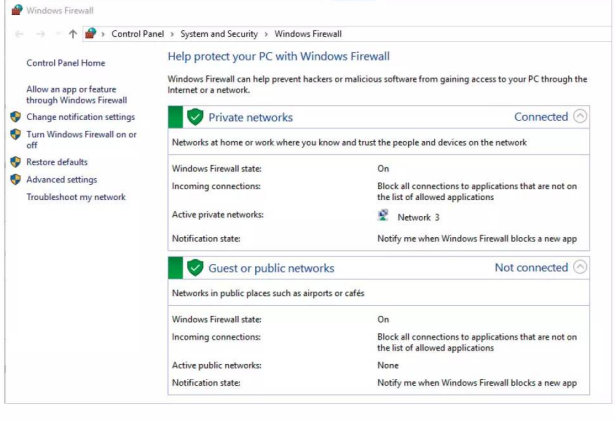
Getting to Know Your Firewall

Generally, there's little need to ever configure the Windows firewall. However, getting to know how it works and improving it is part of being more security-conscious. Here's some tips on how to manage it better.

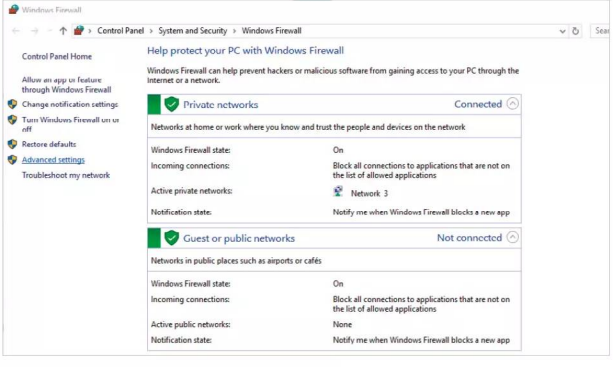
STEP 1 You can open the main Windows firewall console window by clicking on the Windows Start button and entering firewall into the search box. Click the returned link, Windows Firewall Control Panel, to launch it.



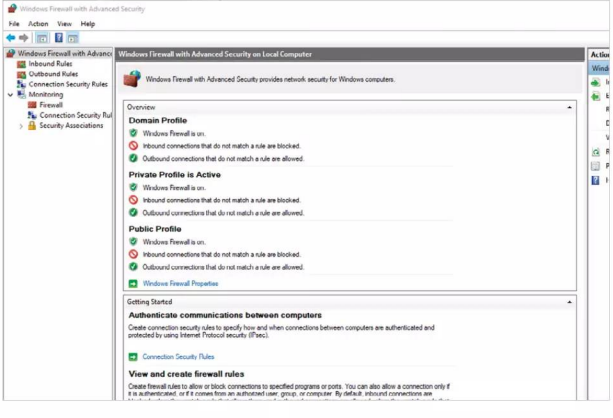
STEP 2 The Windows firewall console window starts by detailing the basic status of the firewall. It should be On by default, unless you've installed a third-party security suite which contains its own firewall. There are two kinds of network listed, Private and Public. Private is for home or work, whereas Public is for cafés and the like.



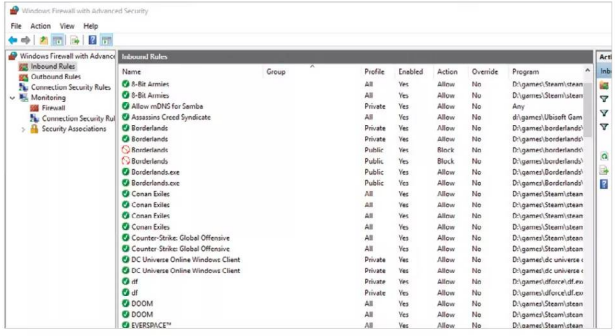
STEP 3 Down the left-hand side are some links that will help you configure and improve the firewall, as well as turning it on or off (which isn't recommended under any circumstance other than the installation of an improved third-party firewall). To begin with, start by clicking on the Advanced Settings link.



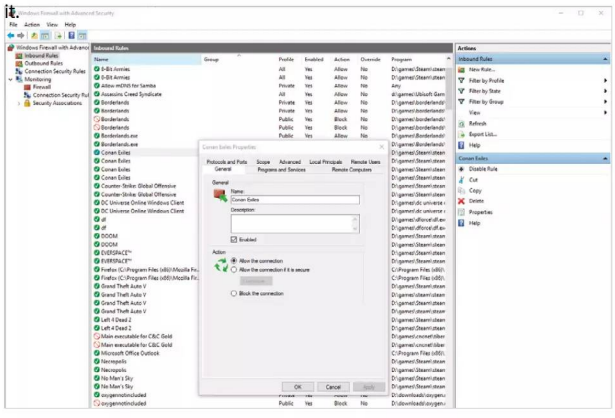
STEP 4 The Advanced Settings link launches a new console window. This new console defines the inbound and outbound rules for the entire system and its installed programs and applications. You can set authentication rules between computers, view and create new firewall rules, view the current firewall policies and even monitor what's being blocked in realtime.



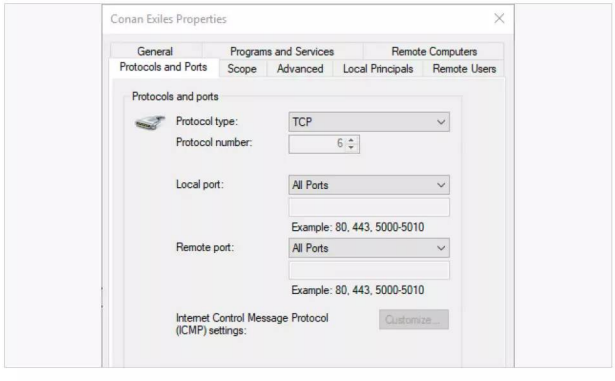
STEP 5 Click on Inbound Rules to the right-hand side of the main console window. This will list the current rules that allow traffic into your computer and to the applications that require it. For example, in this screenshot there are rules for various games that allow multiplayer interaction and the ability to 'talk' to the game server as well as install updates.



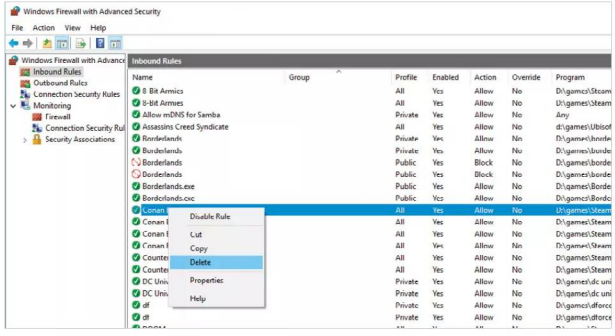
STEP 6 These rules are automatically entered into the firewall when you install the program, game or app. When you install a program you're required to accept and authenticate the process, clicking on Yes to start the installation. This level of administrative access also allows entry of the program into the firewall. Pick one of the entries and double-click



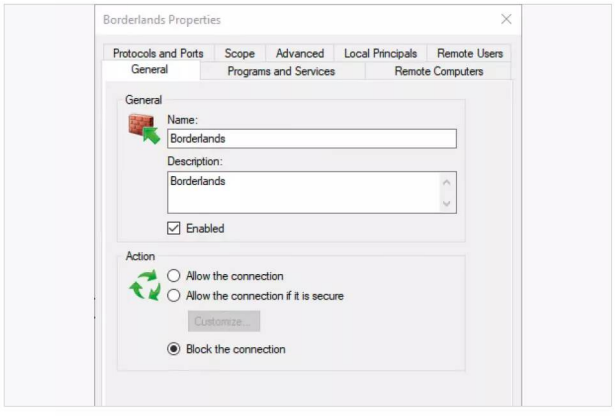
STEP 7 The properties of each firewall entry allow a greater degree of control for that particular program. You can change the name of the entry, allow or block the connection, define the physical location of the program on your computer, allow access to the program from remote computers, set the protocol and port number it uses and even which network controller to use.



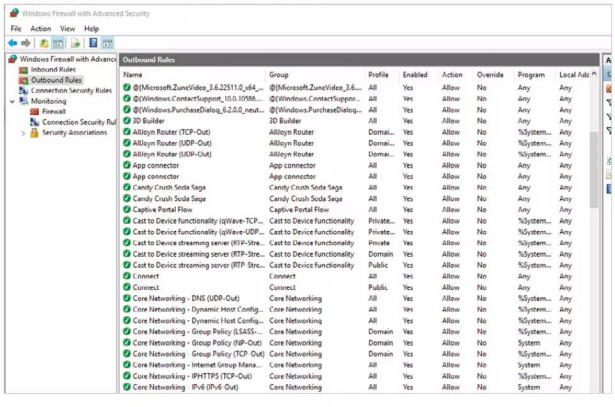
STEP 8 Sometimes, uninstalling a program doesn't automatically remove it from the Windows firewall. The exact reasons why are varied but to help improve the efficiency of the Windows firewall, whenever you remove a program from your system, it's worth checking the firewall to see if its entry has been deleted. To delete an entry, right-click then select Delete from the menu.



STEP 9 You may not want to delete a rule as it could be used later or if you reinstall the program and it fails to recreate the firewall entry. The recommended process then is to block the rule from communicating with the outside world. To do this, double-click the rule and from the General tab click the Block the connection button.

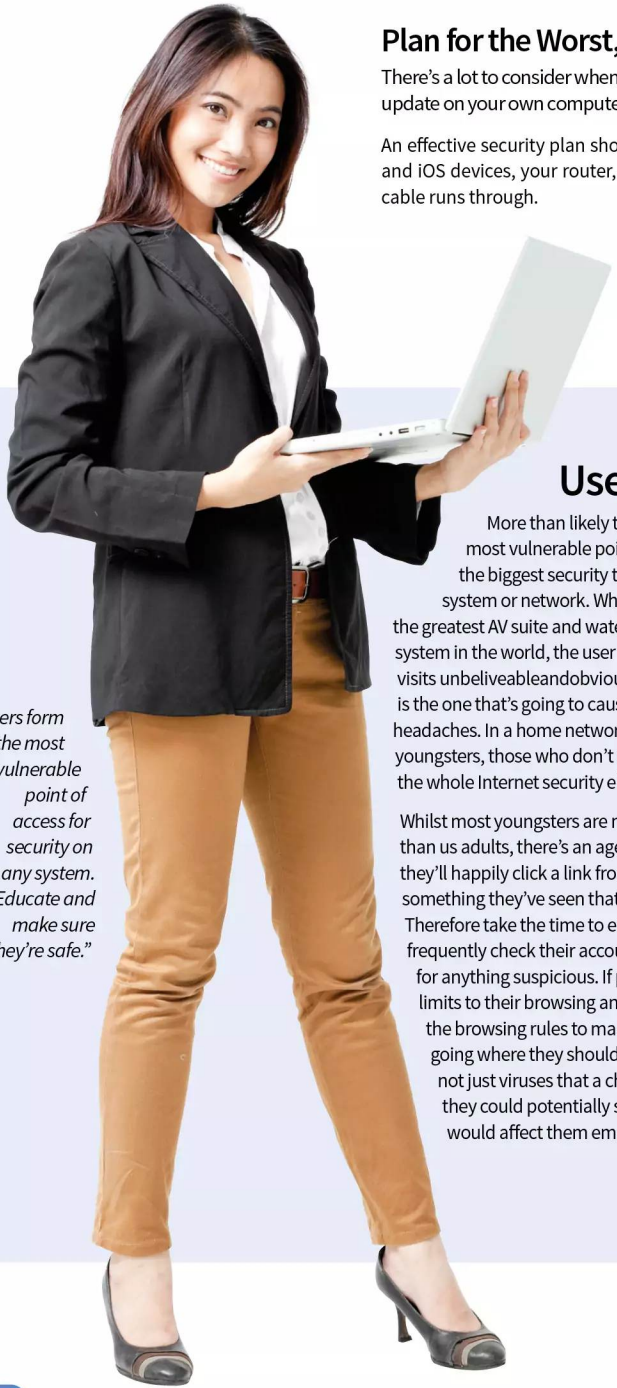


STEP 10 Similarly, the Outbound Rules link will detail the various programs that are allowed to communicate from your computer to an external destination. It's good practise to familiarise yourself with the rules of the firewall, as a rogue program will need to set a rule to communicate. You can then block that rule and stop the threat from reporting back.



Creating a Security Plan

A security plan will help you form a better strategy when it comes to tackling your Windows and home network security. A good plan will help keep on top of backups, updates and possible areas of weakness that malware or hackers can exploit.



Plan for the Worst, Hope for the Best

There's a lot to consider when coming up with a good security plan. It's not just a case of occasionally checking for an OS update on your own computer, you have to take into account other computers and the entire network.

An effective security plan should encompass the whole of your network, which includes Windows computers, Android and iOS devices, your router, any powerline adapters, Wi-Fi coverage, access passwords and even where the Ethernet cable runs through.

It may sound a little extreme but like most checklist-type scenarios it can be as in-depth as you like. However, it's worth at least considering some aspects of the home network and overall security before starting a plan.

Users

"Users form the most vulnerable point of access for security on any system. Educate and make sure they're safe."

More than likely the 'user' is the most vulnerable point of access and the biggest security threat to any system or network. Whilst you can have the greatest AV suite and water-tight security system in the world, the user who carelessly visits unbeliveableandobviouslyfakedeals.com is the one that's going to cause you the most headaches. In a home network that's often youngsters, those who don't quite understand the whole Internet security element.

Whilst most youngsters are more tech-savvy than us adults, there's an age range where they'll happily click a link from a friend or something they've seen that looks cool. Therefore take the time to educate and frequently check their accounts or computers for anything suspicious. If possible enforce limits to their browsing and regularly update the browsing rules to make sure they're not going where they shouldn't. Remember, it's not just viruses that a child can download, they could potentially see something that would affect them emotionally.

Updates

Obviously a must-have section of a good security plan is to regularly check for system and program updates. Thankfully, Windows and most security suites will run an automatic check whenever the system is powered up and connected to the Internet. However, there's always some point where an update failed to initialise for some reason or another. Therefore, it's often best to manually check.

Consider too checking for updates for the most frequently used programs. Microsoft Office, GIMP, your browser and even games will inevitably have an update available which can enhance, protect and improve the security of the program. After that, make sure that the other installed programs on the system are up-to-date too, as it's best to make sure there's few weaknesses as possible.

Programs

It can be difficult to keep track of what programs are installed on a system but it's not impossible. If you're serious about the security of your home network and its systems, then taking stock of what programs are installed on each system is worth doing.

Running through a checklist of installed programs you may notice one that shouldn't be there. A quick lookup of the program may reveal that it's a popular backdoor for hackers to get into a system and the attached network. That being the case, it needs to be removed and any firewall entries checked and disabled.

Routers

The family router is the first point of access for anything malicious on the network, since it's the gateway to the outside world. Make sure that the router software is up-to-date and that it's using the best possible wireless security standards and encryption.

It's also beneficial to make sure that the router's admin password and access passwords are hidden from sight. It doesn't take much for someone to look through the front window and make a note of a router password that's carelessly on show for all to see. Consider too, that not all visitors to your home are going to be chivalrous towards viewing your network password.

It's also worth tracking the range of the wireless signal from the router. By installing and using a good Wi-Fi scanner on a mobile device you can tell where the Wi-Fi signal from your router lies beyond your home. Whilst it's good to have a powerful signal, it won't take much for someone to sit nearby with a laptop (or a neighbour) and hack into your network. A Wi-Fi analyser will help you determine the best placement for security and more efficient use of the signal.

Passwords

It's not common for a home user to frequently change their password to the same degree as would an office worker but it's certainly something worth implementing. Using a combination of a good password manager and generator, you can set a 30-day password limit for all users and their access to the sites they visit.

It might sound like an awful lot of hard work on the part of everyone involved but weak passwords and the same password being used across Facebook, banking and gaming is a huge security vulnerability.

Backups

We'll cover backups in a few pages time but for the meantime though making sure that each account and computer is regularly backed up can take much stress out of a security situation. If you're unlucky enough to catch a virus or other malware, or are unfortunate enough to be hacked, you'll need to act quickly to prevent any loss of personal information. This usually means wiping your computer completely.

Having a good and reliable backup solution will help you recover your valuable data in no time, should you ever need to wipe everything or all your data is compromised through malware. It's also worth thinking of investing in a fireproof safe to store your backups along with cloud options for off-site backup security.

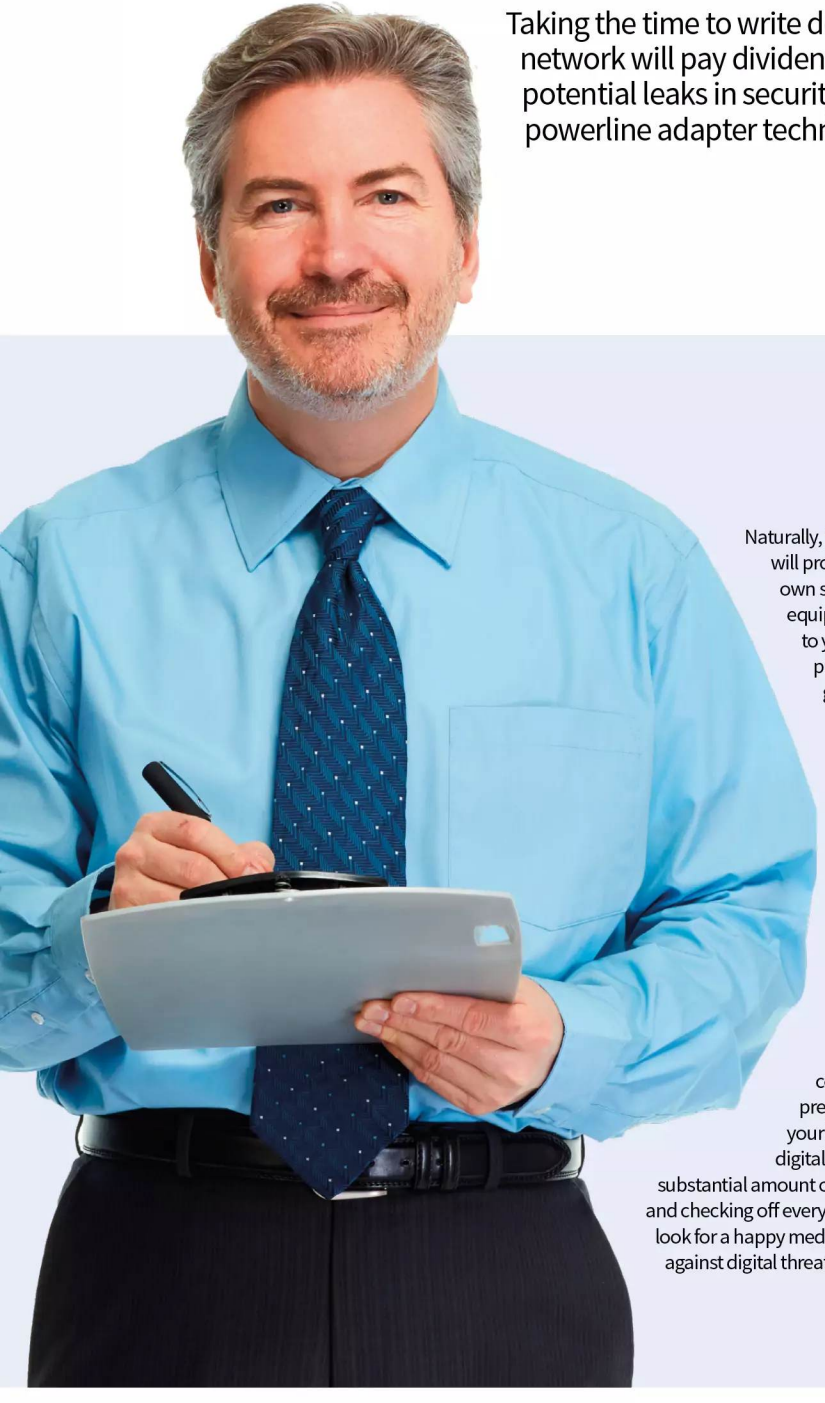
Cabling

It's not always something you need to check but ensuring that the home's Ethernet cabling is secure is an essential element to network security. For example, if you live in shared accommodation, it's possible for a neighbour to be able to be able to connect to your Ethernet cable and steal your bandwidth or gain access to your network resources.

If you can implement all or just some of these elements into your plan, you will be well on the way to making sure that your home network is as secure as possible, without becoming too paranoid over potential threats from outside sources. After all, you lock your doors when you're not at home so why shouldn't you lock your network too.

Windows Security Checklist

Taking the time to write down an effective security plan for your home network will pay dividends in the long run. With it you're able to spot potential leaks in security, secure your home network, Wi-Fi and powerline adapter technologies, and ensure digital peace of mind.



Naturally, this is just our example and will probably be different to your own setup and depending on the equipment you have available to you. For the sake of this publication we've taken a more generic approach but it's worth using it as a foundation from which you build your own, personal and unique checklist. Your checklist can be as intricate as you like, detailing specific hardware or software on one or all your computers, devices and so on, that needs to be updated regularly. Just remember though, there is a point where you can become a little too security conscious. Whilst it's great to be prepared for anything, and run your home network like a veritable digital Fort Knox, it can take up a substantial amount of your time applying patches and checking off every item on the list. Therefore, look for a happy medium, whilst remaining vigilant against digital threats.

We've come up with a template security checklist that you can use to create your own, for your

> **Plan Ahead**

home network. Remember to tick each section and remember to keep checking regularly and alter it as new devices are added.

Checklist

Router

Make sure that your router's admin password and access passwords are in a secure, unviewable place. So visitors can't see them when they come into your home.

Wi-Fi Security

Login in to your router and check that the Wi-Fi is using WPS2. Then check the currently attached devices for any anomalies. If you use any other form of router security, double check it's still functioning as updates can reset routers.

Wireless Positioning

Using a Wi-Fi analyser on your phone or tablet, measure the impact of the wireless signal from the router. If it's reaching out into the street and not so much the rear of the house, then consider moving it. Keep an eye on the signal power and weak locations.

OS Update

Check for any operating system updates on all the computers and Windows mobile devices that connect to the home network.

Security Suite Update

Run a similar update check on any antivirus clients, VPN clients or other third-party security programs and applications.

Program & App Update

Run any update checks on frequently used programs and applications. After that, run as many updates on other installed programs on all your computers.

Installed Rogue Program and App

Check each computer on the network for its list of installed programs. If there's anything in there that doesn't look right, research it and remove it if necessary. Make a note of the programs installed (as a screen shot or physical note) and compare them with each frequent check.

Password Reset

Set a regular, usually 30-day, password reset. Each individual user should be able to reset all their passwords for every site they visit and make sure that the passwords they're using are strong. Use a password manager and password generator if needed.

Firewall Integrity

Check that the firewall on each computer, and potentially any devices, is up and running and that there's no rogue programs within the inbound and outbound rules set.

Backup Important Files

Make sure that each computer and device is regularly backed up. We'll cover how to effectively back up a Windows computer later on. Back up important documents and keep the backup copy somewhere safe; consider purchasing a fireproof safe.

What is a Sandbox?

Sandboxing is an important security technique that's used by companies and individuals the world over. It's not something the average user will normally come across but you can guarantee that every piece of software you use has been sandboxed at some point in its development.

Playing in the Sand

Everyone from software developers and security experts to the hackers themselves will use a sandbox environment to help build and test their products; so what exactly is a sandbox?

Just as the name suggests, a sandbox is a place where you can do something without it affecting the surrounding area: visualise a sandbox in the middle of a garden. In digital security terms, this means a sandbox is a tightly controlled environment that's isolated from the main operating system where a person can test or analyse software and its impact on a virtual system.

The sandbox can be one of a number of implementations: web based, operating system based, program based, network based or even emulating interaction with the Internet. There are countless more examples, each depending on what exactly is being tested and what functions are required to complete the test.

For security, a sandbox is usually an extremely isolated environment that doesn't have access to anything on the company network, or any contact with a host machine. Here the security expert is able to conducts tests on untrusted pieces of code, known malware and viruses and even website content. Should those tests reveal something nasty within, the security expert is able to work their magic and develop a fix that can be further tested and finally deployed to the company's servers, where it's downloaded as updated virus definitions by the security suites and applied to a customer's computer.

Imagine that from the point of view of a hacker, then. The hacker has developed a particularly nasty piece of code that could bring down government agencies and cause widespread panic among the global digital community; they're hardly going to test it on their own computer. They need to create a sandbox environment whereby they can trigger the malware, ransomware or whatever, and let it run its course. In the meantime they can run through various procedures to try and wipe the malware, as a security expert would, to find any weaknesses. Once they've perfected the malware and wiped out any perceivable vulnerabilities, they can then happily upload it to the Internet and sit back as the world is infected with their code.

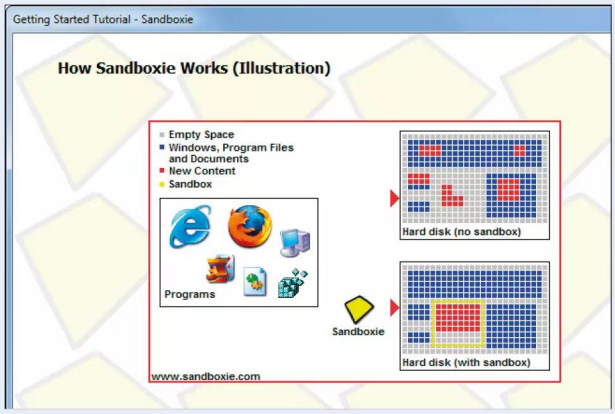
It's not always the testing of malicious code that's associated with sandboxes. For example, the words you're reading now were written using Office 365/ Word 2016. Before the product was released by Microsoft, the development team behind Word will have gone through extensive testing, making sure that all the individual components within and that make up Word 2016 all worked. To do so, they will have used a dedicated and separate environment to the one they're using to program on. This specialised environment will have mimicked a real world setup as much as possible, so that when the developer wanted to test something they could compile the code and execute it in an environment that wouldn't affect their normal day-to-day workplace.

The often severe lockdown of a sandbox system does make it difficult to emulate what the average user may be using. The standard desktop computer has many different elements, both hardware and software, that work together to make up the computer that you've customised and personalised. A developer, security expert or software tester can never hope to create something that works 100 percent with every Windows desktop system that's out there.

It's generally accepted then that when testing in a sandbox it's advisable to use as common a hardware and software setup as possible. This way, the developer will likely create a program that works on as high percentage of the computers available. Those computers that differ from the norm, and that may require a little more work for the product to install and work on, can then be dealt with through minor patching and bug testing.

So what's this got to do with you, we hear you say. Well, there are ways in which you can create your own sandbox environment to test in. Consider how many times you've downloaded software from the Internet and executed it without even examining how it may affect your computer. How many times do you visit websites and happily click on whatever message may appear without even reading it properly. With your own sandbox environment, you can download and install a piece of software and see how it runs within a test setup without it ever impacting your real machine. If you get into the habit of testing every bit of software in a sandbox first, you'll certainly be glad should the day come you discover a hidden virus in the folds of an otherwise harmless looking program.

> *Using a virtual machine as a sandbox is a great way to test programs for every version of Windows, not just the latest*



"Sandboxie is an environment designed to allow you to test programs without them being installed on your computer."

"VirtualBox is considered to be one of the leading and easiest to use virtual machines, where you can create a sandbox environment to test in."

Running Windows as a Sandbox

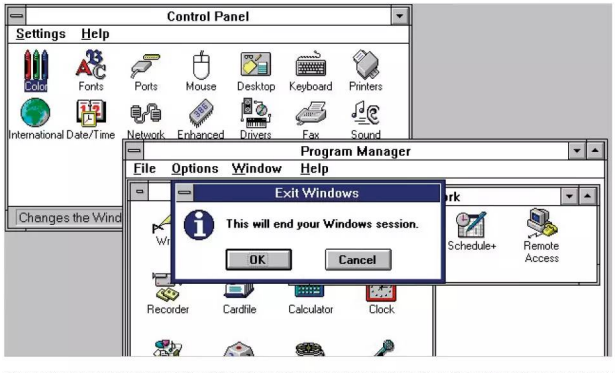
We've already talked about how a sandbox works and essentially what one is in terms of computing and security. However there are many advantages to creating your own virtual sandbox environment. It's not always purely to test suspicious code, as you'll soon discover.

Sand Between Your Toes

If you're still convinced that a sandbox environment can help you out, then read on. We've compiled a list of ten reasons why creating your own Windows sandbox is beneficial to the average user.

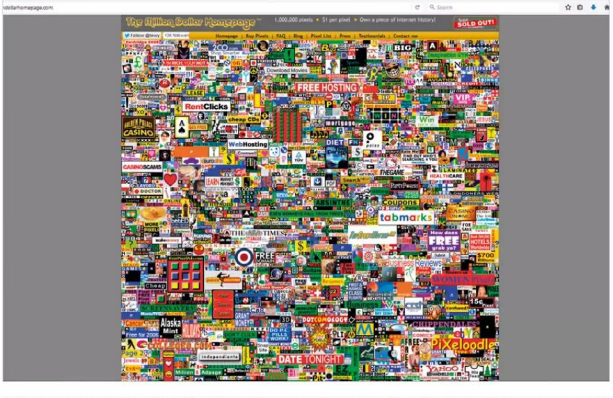
OLD PROGRAMS

Within the Windows virtual sandbox environment you may be able to run older programs that would normally fail, even in compatibility mode, under more modern hardware drivers. Often an older program will look for a specific driver set, if it's too modern then it can fail. Virtual environments use older type drivers by default.



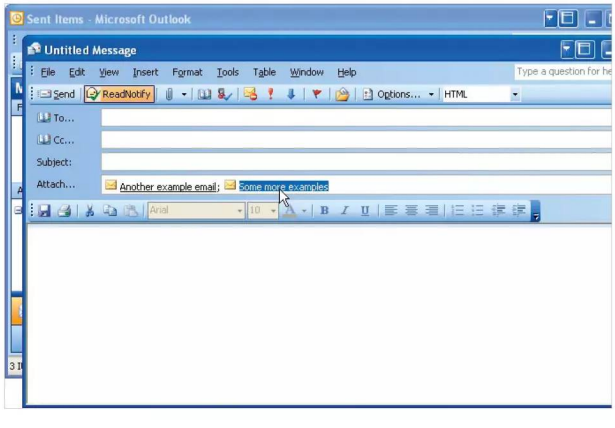
SAFE BROWSING

Within a virtual environment you can browse a site without any of its code being written to the main, host computer. This could simply be cookies and other such relatively harmless additions to sites or it could include data miners and malicious links.



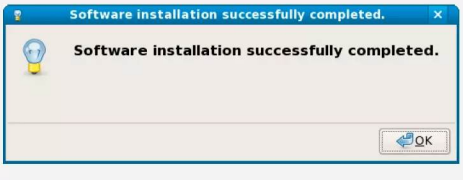
HOST PROTECTION

If you think that a download link or email attachment may contain a virus, then opening it in a safe, virtual environment is the safest bet. Of course, you shouldn't open any unknown email attachments but if you need to, do so in a sandbox. The virus will infect the sandbox and not the host (real) computer.



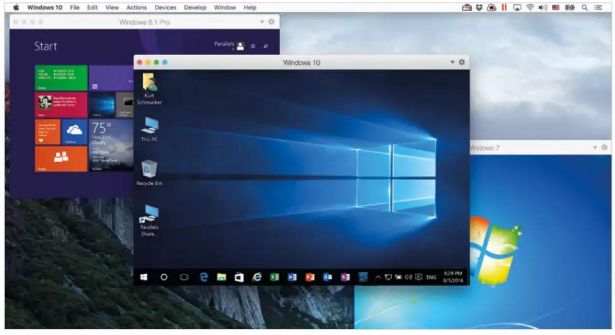
SOFTWARE TESTING

If you're serious about your security and the safety of your home computer, then you should be downloading and installing software in a test environment first before applying it to your real computer. A virtual environment is a great place to see how software works and whether it's worth installing or not.



VIRTUAL OS

The beauty of a virtual environment, such as one created by VirtualBox, is that you're able to run Windows, macOS and Linux operating systems on top of your host operating system, whatever system that may be. You can install Windows within a virtual environment whilst using Linux or macOS, or vice versa.

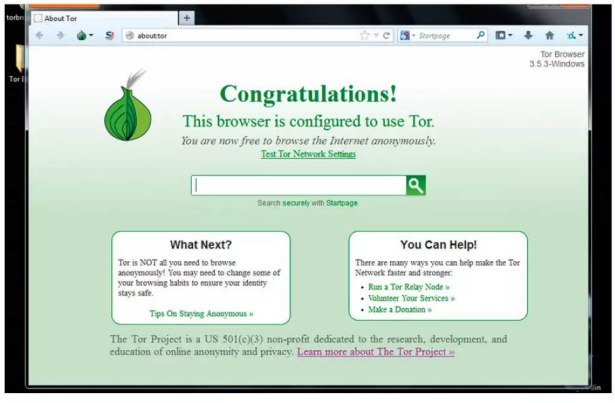


VIRTUAL BACKUP

It is possible to create a virtual copy of a physical machine. This is an excellent way of making sure that the entire machine, that is a snapshot of the OS as it was when copied, is safely backed up and accessible regardless of what operating system you choose to use.

SECURE ANONYMITY

Within a virtual Windows environment you're able to create an anonymity system. By this we mean, you can install a VPN and use the Tor network and surf the Internet without fear of being traced; and what's more, none of it will affect your host operating system.



SAFE DEVELOPMENT

If you're considering developing your own software and apps, then using a virtual environment is an ideal place to test the code as you create it. Should a function you've written have an adverse effect on the OS, then you won't damage your working system.

```
Program Check_Group
  use crystallographic_symmetry, only: Space_Group_Type, set_spacegroup
  use reflections_utilities, only: Hkl_Absent
  use Symmetry_Tables, only: spgr_info, Set_Spgr_Info

  ..... ! Read reflections, apply criterion of "goodness" for checking,
        ! set indices i1,i2 for search in space group tables ...
  ..... ! omitted for simplicity
  call Set_Spgr_Info()
  m=0
  do_group: do i=i1,i2
    hms=adjustl(spgr_info(i)%HM)
    hall=spgr_info(i)%hall
    if( hms(1:1) /= "P" .and. .not. check_cent ) cycle do_group ! Skip centred groups
    call set_spacegroup(hall,Spacegroup,Force_Hall="y")
    do j=1,nhkl
       if(good(j) == 0) cycle  !Skip reflections that are not good (overlap) for checking
       absent=Hkl_Absent(hkl(:,j), Spacegroup)
       if(absent .and. intensity(j) > threshold) cycle do_group  !Group not allowed
    end do
    ! Passing here means that all reflections are allowed in the group -> Possible group!
    m=m+1
    num_group(m)=i
  end do  do_group
  write(unit=*,fmt=*) " => LIST OF POSSIBLE SPACE GROUPS, a total of ",m," groups are possible"
  write(unit=*,fmt=*) "     ---------------------------------------------------"
  write(unit=*,fmt=*) "     Number(IT)      Hermann-Mauguin Symbol      Hall Symbol"
  write(unit=*,fmt=*) "     ---------------------------------------------------"
  do i=1,m
    j=num_group(i)
    hms=adjustl(spgr_info(j)%HM)
    hall=spgr_info(j)%hall
    numg=spgr_info(j)%N
```

FAMILY FRIENDLY

If you have a single-family computer, a virtual environment is a great place for the kids to go without fear of them potentially breaking the system. It doesn't happen often, kids are mostly more tech-savvy than adults but little fingers do have a habit of clicking things they're not supposed to. Virtual environments can be backed up and redeployed easily.

RESTRICTED ACCOUNTS

Again, using children as an example, a virtual child's Windows account can come with all manner of restrictions and monitoring software, to stop them from wandering into the scarier parts of the Internet, such as installing Net Nanny. Again, these controls won't affect the host computer or adult accounts.

Net Nanny

Installing VirtualBox on Your PC

Oracle's VirtualBox is one of the easiest virtual machine platforms for the beginner to experiment on. Within it you can install Windows, Linux and older operating systems, without ever having to alter your main computer's setup.

Going Virtual

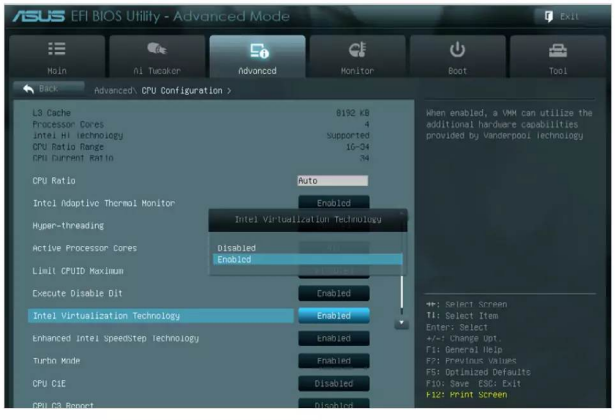
Using a Virtual Machine (VM), will take resources from your computer: memory, hard drive space, processor usage and so on. So make sure you've got enough of each before commencing.

STEP 1 The first step is to get hold of the latest version of VirtualBox. Enter www.virtualbox.org, and click on 'Download VirtualBox'. This will take you to the main download page. Locate the correct host for your system: Windows or Mac – the host is the current, installed operating system – and click the link to begin the download.

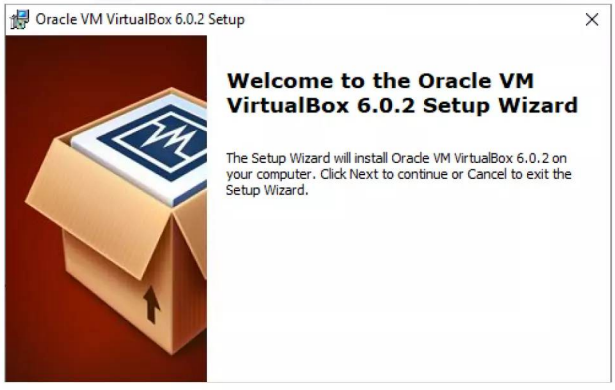
STEP 2 Next, while still on the VirtualBox download page, locate the VirtualBox Extension Pack link. The Extension Pack supports USB devices, as well as numerous other extras that can help make the VM environment a more accurate emulation of a 'real' computer.

STEP 3 With the correct packages downloaded, and before you install anything, you need to make sure that the computer you're using is able to host a VM. To do this, reboot the computer and enter the BIOS. As the computer starts up, press Del, F2, or whichever key is necessary to Enter Setup.

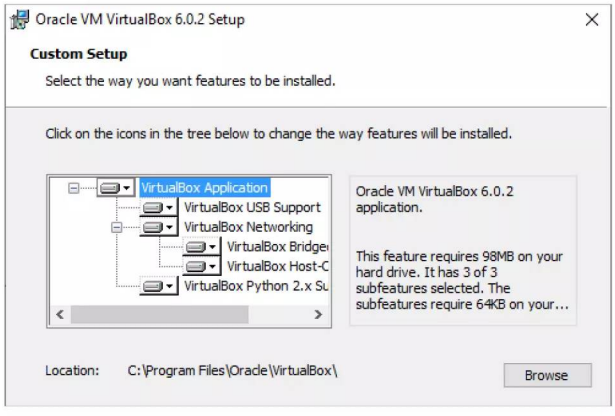
STEP 4 As each BIOS is laid out differently, it's very difficult to assess where to look in each personal example. However, as a general rule of thumb, you're looking for Intel Virtualisation Technology, or simply Virtualisation; usually within the Advanced section of the BIOS. When you've located it, Enable it, save the settings, exit the BIOS, and reboot the computer.



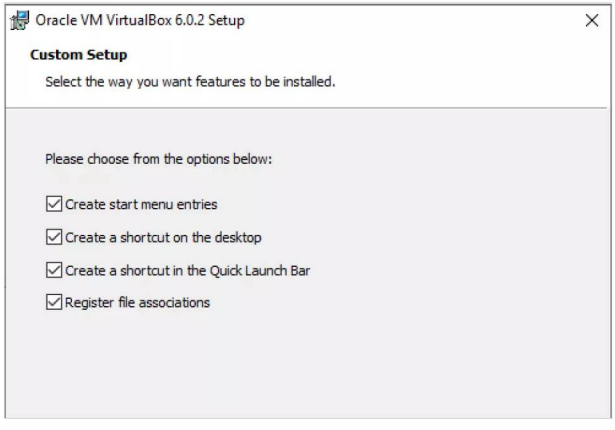
STEP 5 With the computer back up and running, locate the downloaded main VirtualBox application, and double-click to begin the installation process. Click Next to continue, when you're ready.



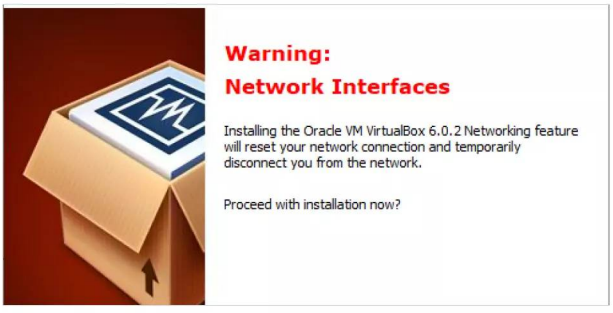
STEP 6 The default installation location of VirtualBox should satisfy most users, but if you have any special location requirements click on the 'Browse' button and change the install folder. Also, make sure that all the icons in the VirtualBox feature tree are selected – none of them have a red X next to them. Click Next to move on.



STEP 7 This section can be left alone to the defaults, should you wish. It simply makes life a little easier when dealing with VMs; especially when dealing with downloaded VMs, as you may encounter in the future. Again, clicking Next will move you on to the next stage.

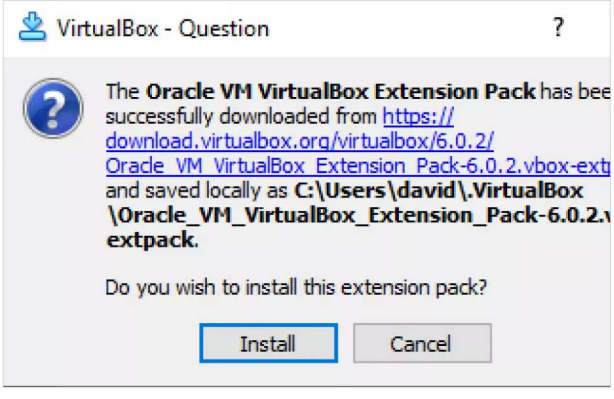


STEP 8 When installing VirtualBox your network connection will be disabled for a very brief period. This is due to VirtualBox creating a linked, virtual network connection, so that any VM installed will be able to access the Internet, and your home network resources, via the computer's already established network connection. Click Yes then Install to begin the installation.



STEP 9 You'll probably be asked by Windows to accept a security notification, click Yes for this, and you may encounter a dialogue box asking you to trust the installation from Oracle; again, click yes and accept the installation of the VirtualBox application. When it's complete, click finish to start VirtualBox.

STEP 10 With VirtualBox up and running you can now install the VirtualBox Extension Pack. Locate the downloaded add-on, and double-click. There may be a short pause while VirtualBox analyses the pack, but you'll eventually receive a message to install it. Click Install to begin the process, then scroll down the next screen to accept the agreement and click 'I Agree'.



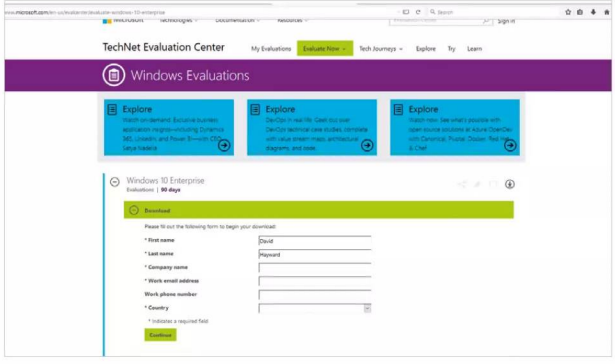
Installing Windows in VirtualBox

Installing Windows within a VM carries with it a clause: you need to make sure you have a valid license. However, if you're testing something then you can use the Windows Enterprise Evaluation image, which will last for 90 days.

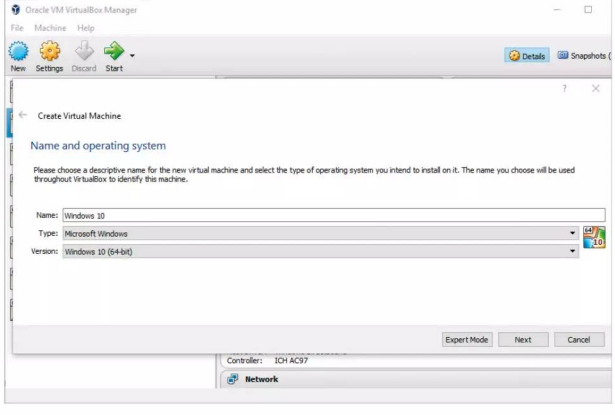
Window Installations

Naturally you might own a spare Windows license to use for the VM but for this tutorial we're going for the 90 day Windows Enterprise Evaluation model. To begin with, browse to https://microsoft.com/en-us/evalcenter/evaluate-Windows-10-enterprise.

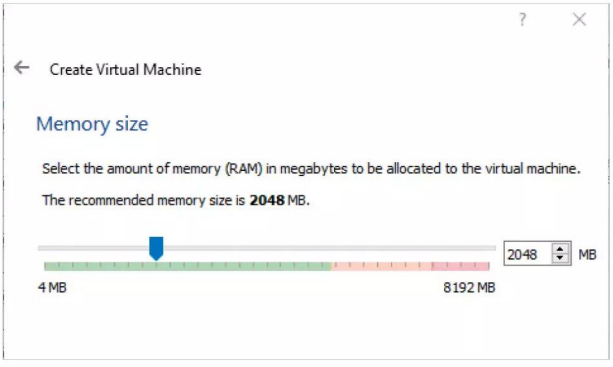
STEP 1 You need to register with Microsoft prior to being able to download the Windows image; simply click the Register button and fill in the required fields. When done, click Continue and choose the ISO Enterprise option, then your language choice and 64-bit, followed by the Continue button once more to begin the download.



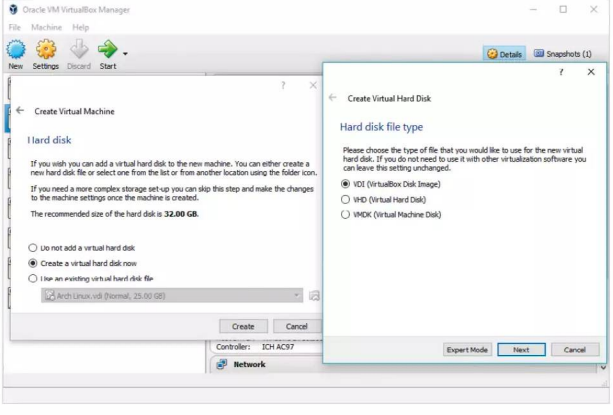
STEP 2 The ISO you're downloading is around 4GB in size, so it may take some time, depending on the speed of your connection. Open VirtualBox and click on the New icon located in the top right of the main VirtualBox window. In the Name field enter Windows, this should automatically change the Type and Version fields accordingly. Click Next when ready.



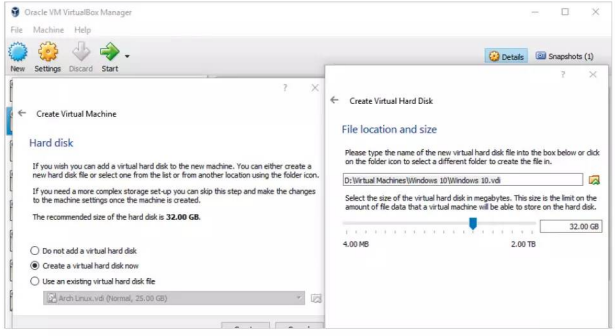
STEP 3 You need to set an amount of memory from your host computer to use as virtual RAM for the VM. Naturally, you don't want to take too much as your computer will suffer due to low memory when the VM is running. Ideally, you need to allocate around 2GB of memory to the VM. Click Next when ready.



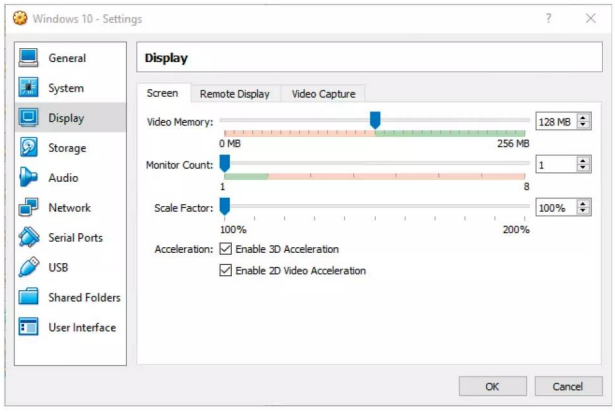
STEP 4 The next section will enable you to create a virtual hard disk, in which the Windows virtual machine can be installed. The default option: 'Create a virtual hard disk now' is recommended, then click the Create button to proceed. The pop-up box will detail the type of virtual hard disk; stick to VDI and click Next.



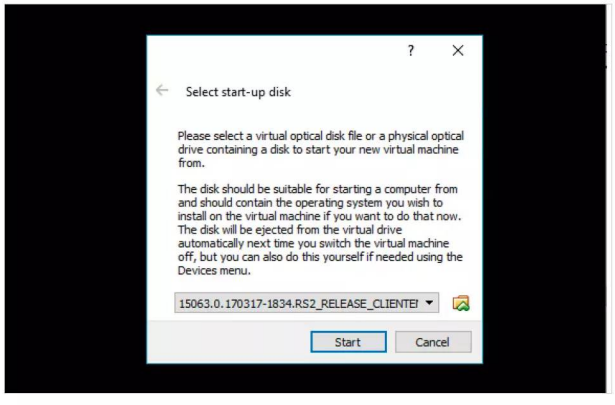
STEP 5 The default Dynamically Allocated option will suffice for this instance, so click Next. VirtualBox recommends that you allocate 32GB of physical hard drive space to creating the virtual hard disk. Make sure your hard drive has enough spare capacity and click the Create button.



STEP 6 The Windows VM is now listed in the available VMs in VirtualBox. Before you begin to install it though, click on the Settings icon whilst the Windows VM is highlighted. In the General tab, click Advanced and enable Bidirectional for Shared Clipboard and Drag 'n' Drop. In Display, enable 3D and 2D Video Acceleration. Click OK to finish.

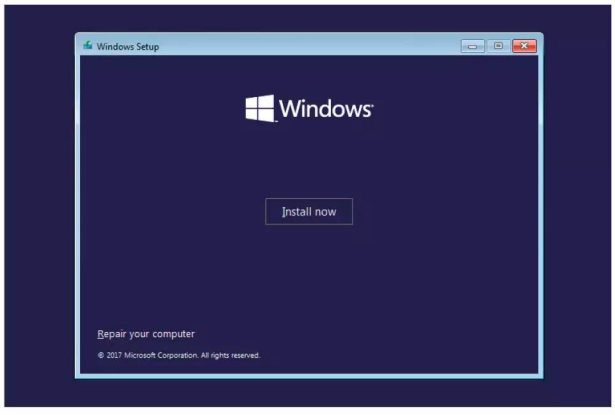


STEP 7 With the Settings console window closed, and the VM highlighted, click on the Start button. This will open a new window, asking for the location of the Windows ISO you downloaded from the Microsoft site in the first few steps. Use the folder icon to locate the ISO and click Open, then the Start button to commence the installation.

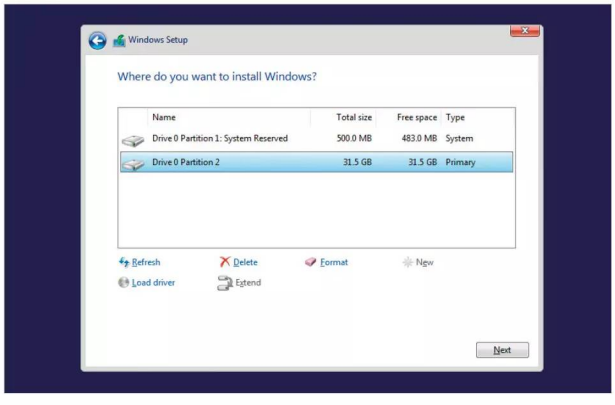


STEP 8 The Windows ISO will now load, and begin the installation process. The first options you need to set are the language, time and keyboard. Set your preferences, although the default is English US to begin with, and click on the Next button when you're ready to continue.

STEP 9 You now have an Install Now option available. Click it to begin the installation, then tick the license agreement box followed by Next. There are two possible options to install Windows, Upgrade and Custom. Since this is a blank hard drive, the Custom option is the only viable mode. Click it to continue.



STEP 10 The drive available will be the 32GB virtual hard disk you created. Click on the New button, then Apply to create a new valid drive that Windows can be installed on. You'll be asked what additional partitions will be created, click OK to accept. Choose the largest partition size and click Next to install Windows.



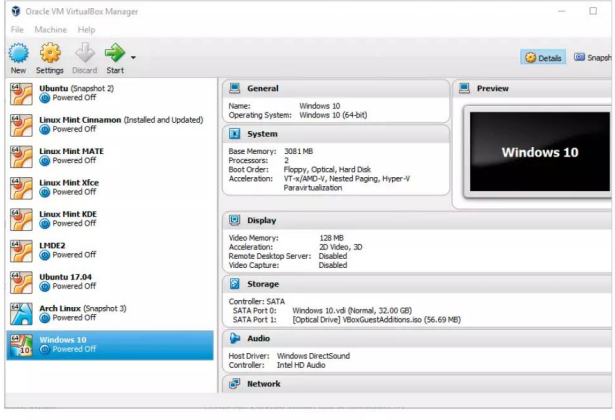
Creating VirtualBox Snapshots of Windows

One day the testing process of a Windows VM will inevitably leave the system in a broken or malware riddled state. You can wipe it and start again but a far better solution is to create snapshots, so you can easily revert to a previous build.

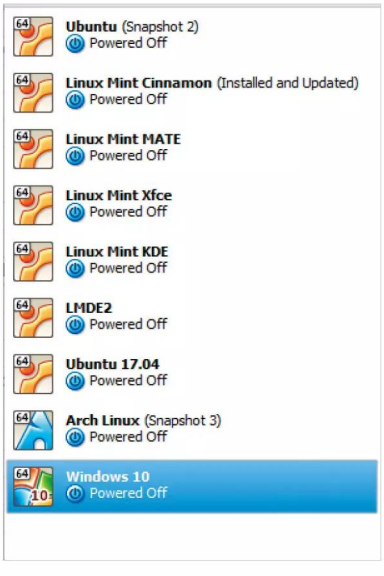
Take a Snapshot

Setting up Windows, installing the drivers, updates and programs takes a fair amount of time. If you take a VirtualBox snapshot, you can return to where you left off in an instant.

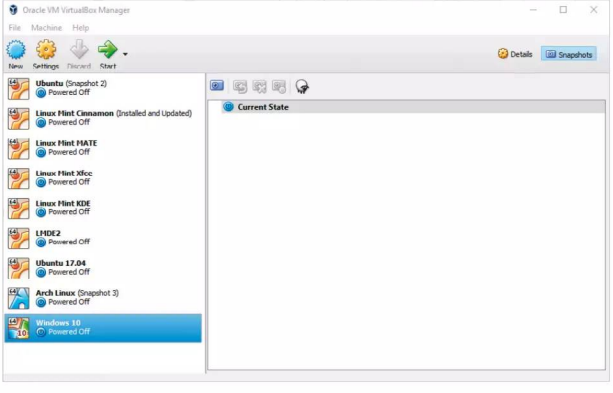
STEP 1 To begin with open VirtualBox. If it's already open, shutdown the Windows VirtualBox image you created. It's not necessary but it's often easier, to ensure the VM is closed prior to creating a snapshot.



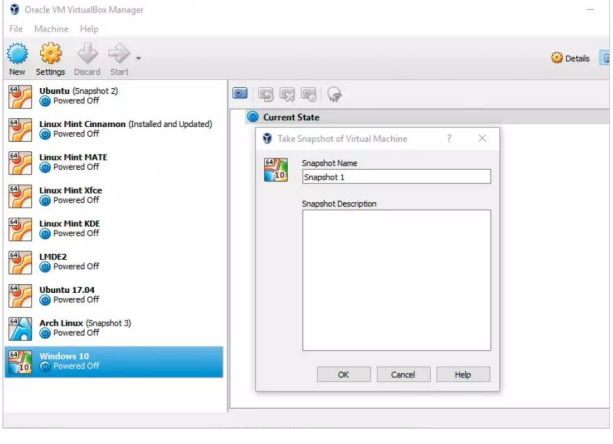
STEP 2 A Snapshot in VirtualBox is simply an image of what the virtual machine 'looked' like at the time the Snapshot was taken. You can make multiple Snapshots and revert to any whenever you wish. Snapshots taken are labelled next to the name of the VM.



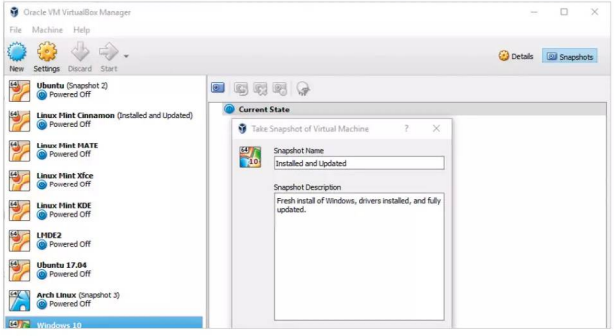
STEP 3 You can see that the state of all the virtual systems is currently Powered Off. To create a Snapshot of the Windows VM, click to highlight the system's entry in VirtualBox, then click on the Snapshots button (it's a camera icon), located to the far-right of the VirtualBox console.



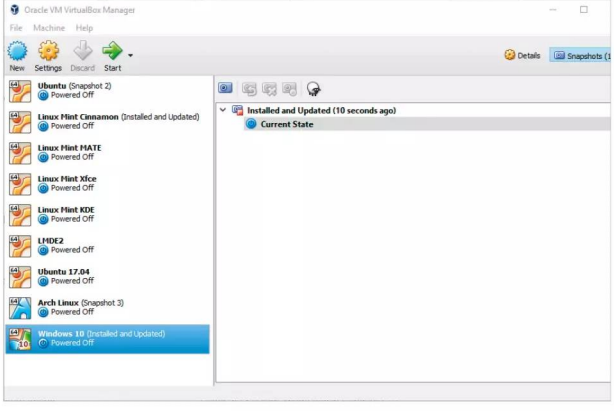
STEP 4 At present there aren't any Snapshots of Windows available. To create one, click the camera icon just above the words Current State, the icon at the opposite end of the sheep icon. This will launch the Take Snapshot of Virtual Machine console window.



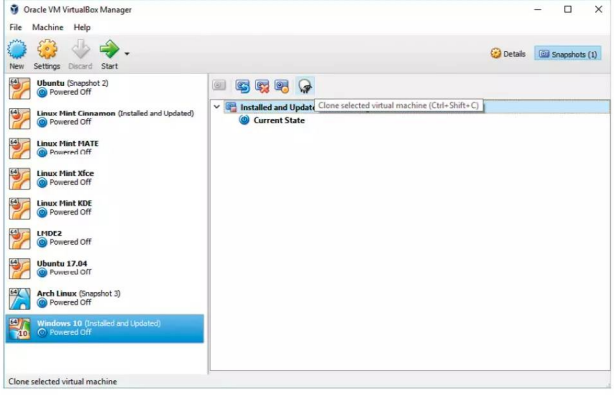
STEP 5 If you want you can name the Snapshot: Installed and Updated for example, along with a description to help identify it easier from the other Snapshots you may eventually end up making. It's not hugely important but if someone else wants to load up Windows, they know which Snapshot to go for. When you're done, click the OK button.



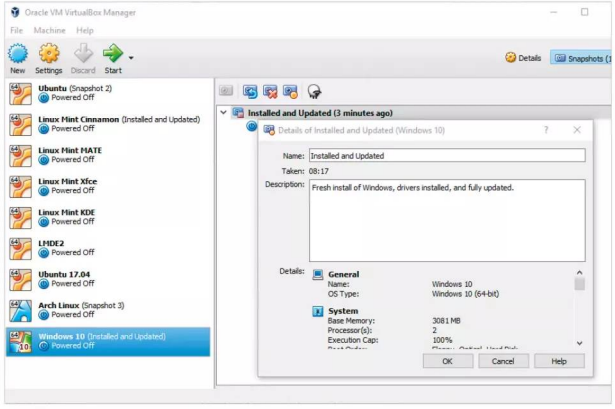
STEP 6 The process happens almost instantly and you're left with an entry in the Snapshots section detailing the named Snapshot, how long ago it was taken and a Current State entry. The Current State is literally its state when you boot it up. With it highlighted, you can take more Snapshots by using the camera icon again.



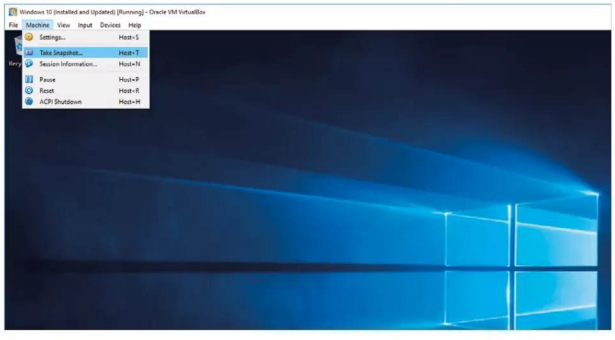
STEP 7 If you click the named Snapshot, you get more options available in the toolbar just above. Here you can Restore a selected Snapshot, if you have multiple entries. You can Delete a Snapshot and view detailed information regarding one; and with the sheep, you can Clone the current Snapshot as a new virtual machine.



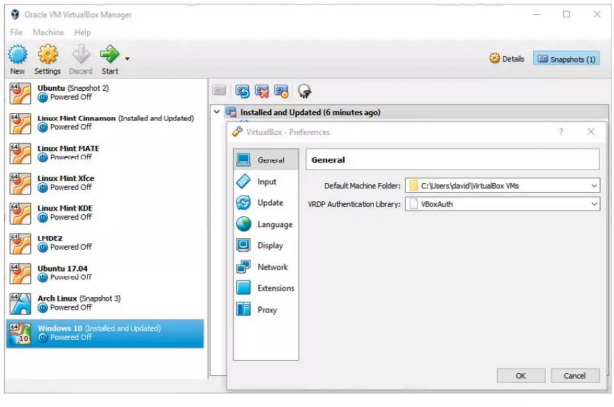
STEP 8 If you click the Details of the named virtual machine icon, the one next to the sheep, represented with an orange circle, you can view the VirtualBox settings of that particular Snapshot. This way you can assess any issues that may arise with other virtual machines; here you can see which settings worked and which didn't.



STEP 9 You shutdown the guest system, as mentioned in Step 1, but VirtualBox guest doesn't need to be shutdown in order for a Snapshot to be taken. For example, prior to installing an experimental program, click the Machine entry in the VirtualBox top menu bar and choose Take Snapshot. The process works the same way as in Steps 4 onward.



STEP 10 Each Snapshot taken can easily be reverted to, cloned, deleted and so on. However, Snapshots are stored by default in the Users/username/VirtualBox VMs folder in Windows. If you've only a limited amount of space on your C:\ drive, you may want to set the path to a bigger hard drive in the File > Preferences option in VirtualBox.



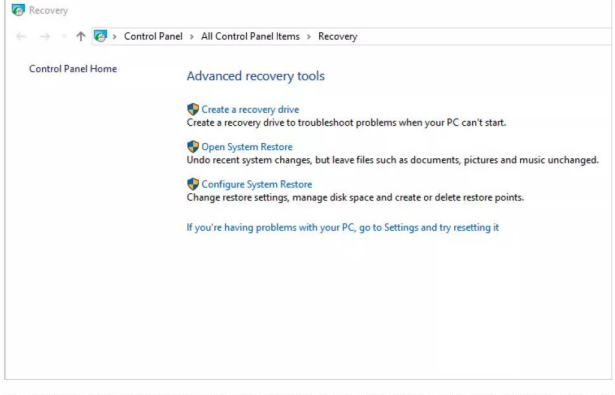
Create a Windows Recovery Drive

Since Windows 95, Microsoft has offered users the ability to create a recovery drive, which is used to help troubleshoot a Windows PC that is failing to boot, by presenting various options. If you haven't done so yet, you ideally should have created a Windows recovery drive.

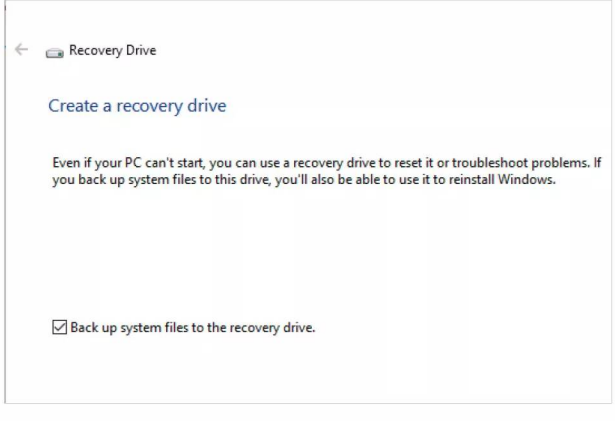
Time to Recover

You need an 8GB USB drive minimum, in order to successfully create a recovery drive. It wipes the contents off the drive and you won't be able to use it for anything else, so make sure it's labelled and stored in a safe place.

STEP 1 Insert the USB drive into your PC and close the Explorer window that opens upon insertion. Click the Windows Start button and type recovery, then click on the Recovery Control Panel. In here you can see several options available; you want the first, Create a recovery drive.

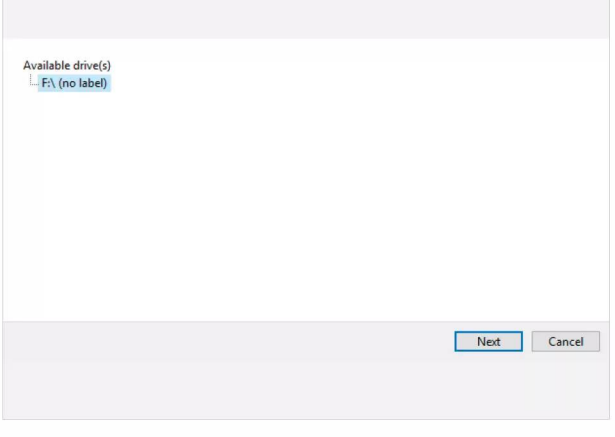


STEP 2 Click the Create a recovery drive link and accept the UAC authentication message that pops up. First, there's the option to backup any important system files to the recovery drive, alongside the usual recovery options. This is a good idea as it can replace these vital files in the event of a boot failure. Click Next to continue.

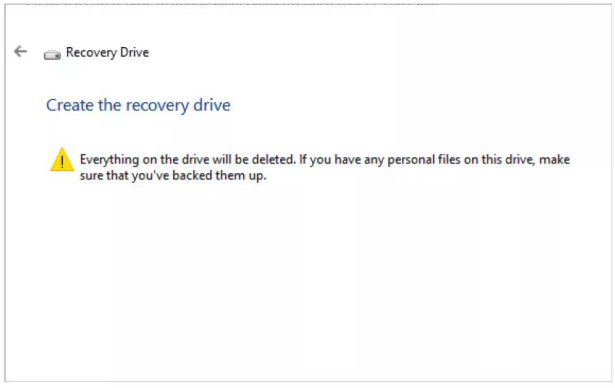


STEP 3 There's a short wait as Windows analyses the available locations where it can install and create the recovery drive. Eventually, providing you inserted the 8GB plus USB stick prior to starting the process, you're asked to select the destination from those Windows has discovered.

STEP 4 In the example we have here, there's just one possible location, the F:\ drive. If you have more than one possible destination available, make sure that you're selecting the correct USB drive for your recovery drive. When you're ready, click on the Next button.

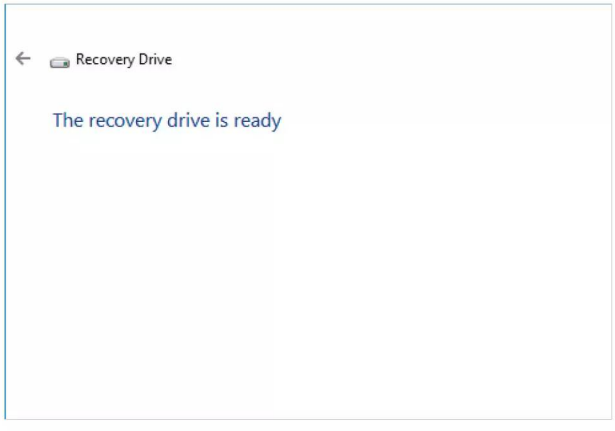


STEP 5 Before committing to creating the recovery drive, Windows will offer one final warning. Remember, everything that's currently on the USB stick you chose as the recovery drive will be erased during the process of creating the drive. If you have any files stored on it, make sure they're backed up to another location.

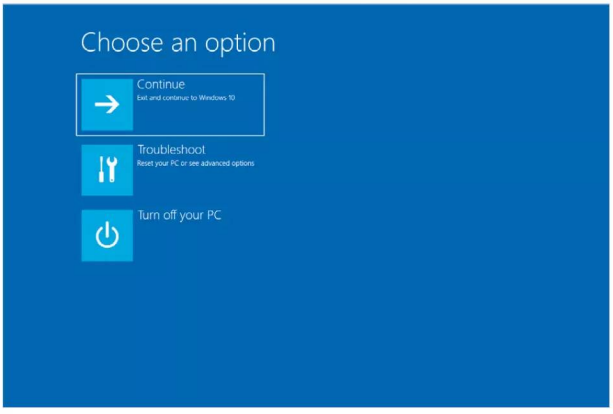


STEP 6 When you're ready click on the Create button to start the process. It may take some time, depending on the speed of the USB stick used, as Windows prepares, formats and copies the utilities and files over to the USB recovery drive.

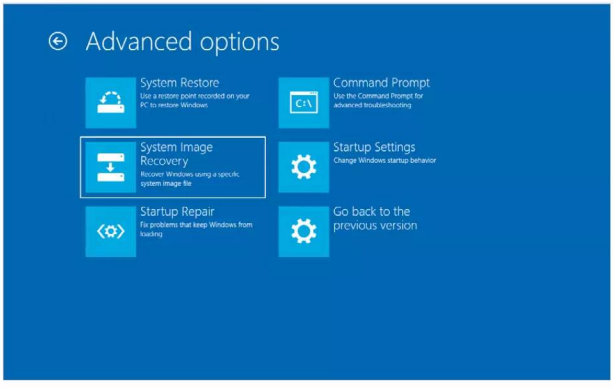
STEP 7 When the process is complete, you receive a recovery drive is ready message. The only option available to you is to click the Finish button. This will close the recovery drive window and return you to the Recovery console.



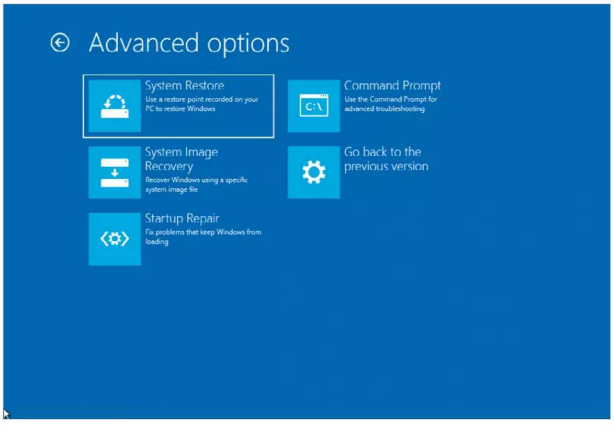
STEP 8 Store the drive in a safe place, as it can restore vital system files should anything ever go wrong with your system and leave it unable to boot. Should something go wrong, you see the Windows safe mode boot options when you try and power up your computer.



STEP 9 From the safe mode boot options, choose the Troubleshoot tile followed by Advanced Options. From there you can choose the System Restore and System Image Recovery options along with your rescue drive to help you recover Windows.



STEP 10 Alternatively, set the BIOS to boot to the newly created recovery drive and follow the onscreen instructions to launch the recovery method. Start by choosing your language, then select the Troubleshoot option and then opt for one of several recovery options.



How to Back Up Windows

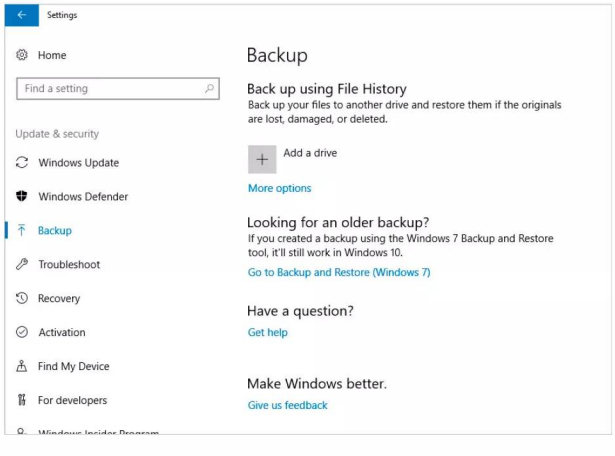
Even with the greatest possible cyber protection in the world guarding your computer, there's still a chance something could go wrong. It might not even be malware-related; a broken hard drive or other component can cause as much grief. Therefore, you need a good backup.

Backing Up

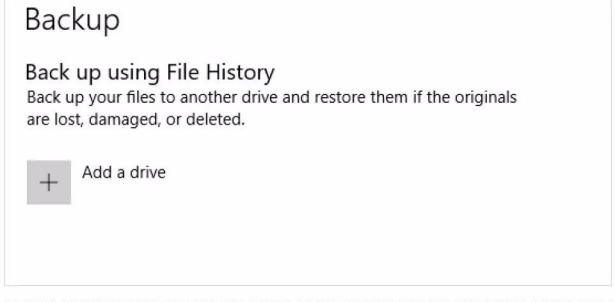
Computers are unpredictable beasts, so you need to make sure that all your files and important data are securely backed up and more importantly, you're able to restore them easily. Thankfully, it's a straightforward process.

STEP 1 Windows has, since its early days, featured some form of backup tool. Windows was launched with the File History backup tool, which is a simple to use tool to ensure stable and regular backups of important files are made. Start by clicking on the Windows Start button and selecting Settings from the menu.

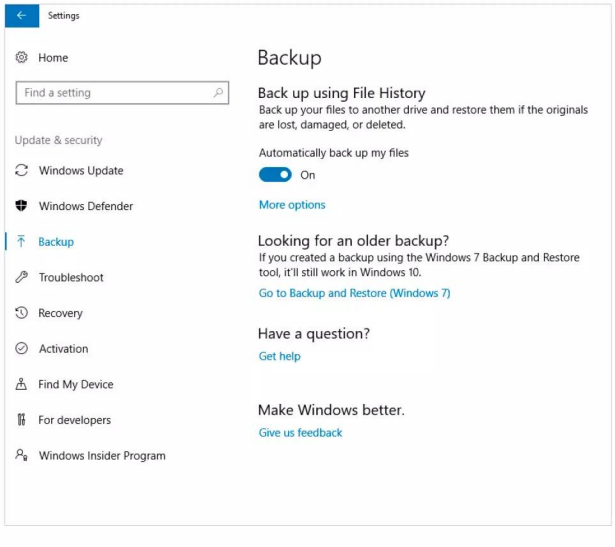
STEP 2 Once in the Settings console, click on the Update & Security icon, followed by the Backup option from the menu on the left. You can see a number of possible options before you: Add a Drive, More options, Go to Backup and Restore (Windows 7), along with help and feedback links.



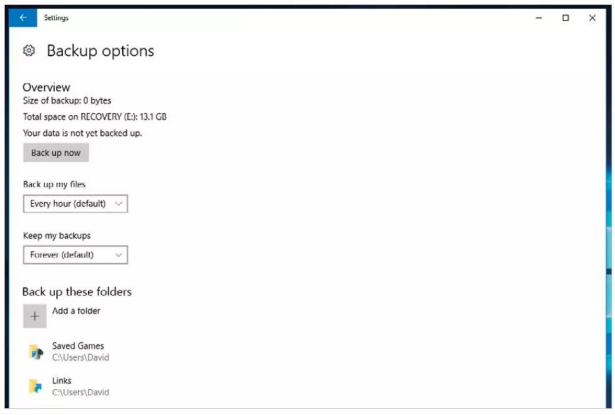
STEP 3 Ideally you need to insert a reasonably sized USB stick or use a second hard drive in your computer. If you have a USB stick, insert it now, or if you own a second hard drive power off the computer and install it and boot back into Windows. Once done, click the Add a Drive icon.



STEP 4 Windows will search for any capable drives on to which it's able to back up your files. When your drive or USB device is displayed, click the drive link. Notice that an 'Automatically back up my files' switch button has appeared where Add a drive once was.

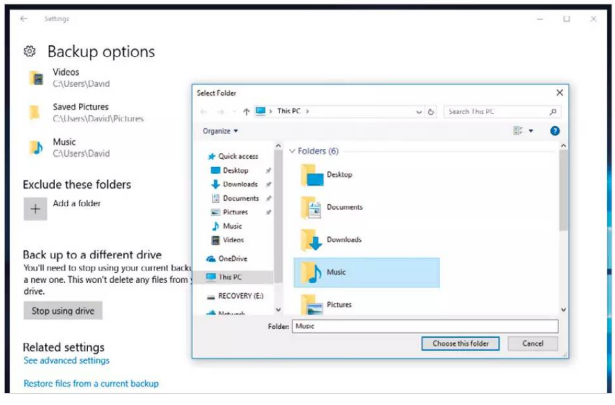


STEP 5 From here, click on the More Options link that's under the switch button, this will open the Backup Options console. This section details the backup schedule, the location and which folders will be included in the backup; and for how long Windows will retain your backed up files.

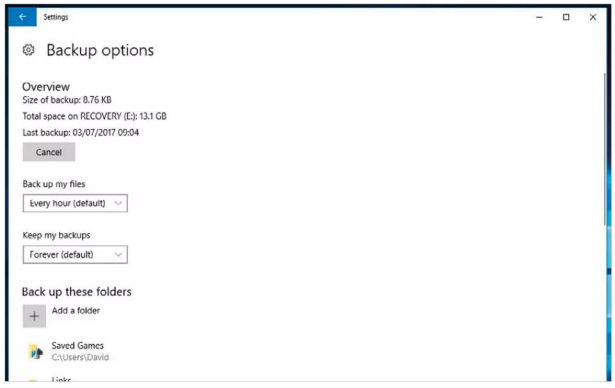


STEP 6 If you scroll down through the Backup Options console, you can see that the entirety of your user folder within Windows has been added by default. This includes the Music and Videos folders, as well as Searches, Camera Roll, Contacts, Favourites and so on.

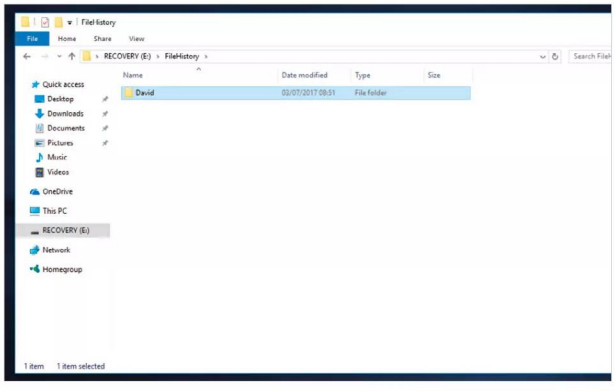
STEP 7 At the bottom of the console window you have the options to stop using the selected drive and to Exclude any folders from the default. If you don't want to back up folders for Music, Videos etc., click Add a folder on the Exclude these folders icon, then pick the folder to exclude and click the Choose this folder button.



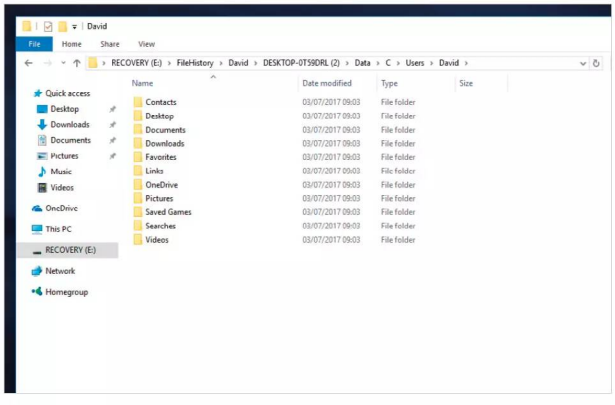
STEP 8 When you're ready to start backing up, you can click the Back up now button to the top of the Backup Option console window. Alternatively, you can wait for an hour when the default schedule kicks in. Obviously, depending on the size of the files within your backup folders this could take some time.



STEP 9 The backed up files will be stored on the chosen backup drive, within a folder called FileHistory. Inside that folder will be the specific user folder, so if you use File History backups for more than one user, their user names will be listed here too.



STEP 10 Drilling deeper into the folder layers reveals more default folders, containing important XML data that Windows uses to store the chosen options. You can find the actual files that have been backed up in the Data folder, laid out in the same folder structure as on your system, i.e. C > Users > Name > Documents etc.



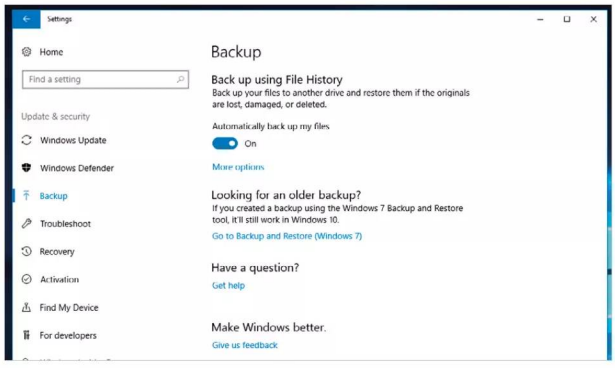
How to Create a Windows System Image

Backing up your files is perfectly fine but in the event of having to wipe your hard drive and start again, getting everything back in order can be time consuming. However, creating a system image means you can almost instantly restore the entire system without needing to rebuild Windows.

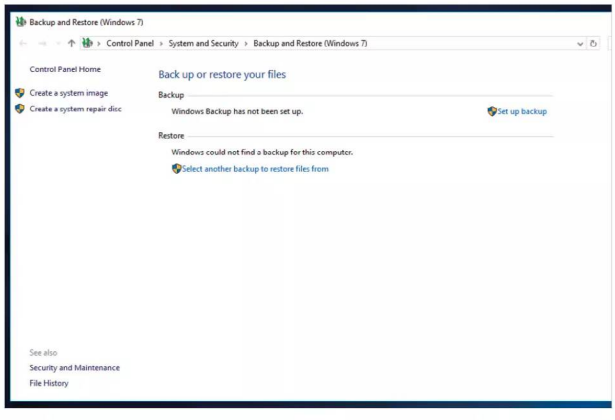
System Imaging

A system image works in much the same way as the VirtualBox Snapshots. You're essentially taking a snapshot of your entire system, which can then be restored quickly. Saving you having to reinstall Windows, all your programs and data.

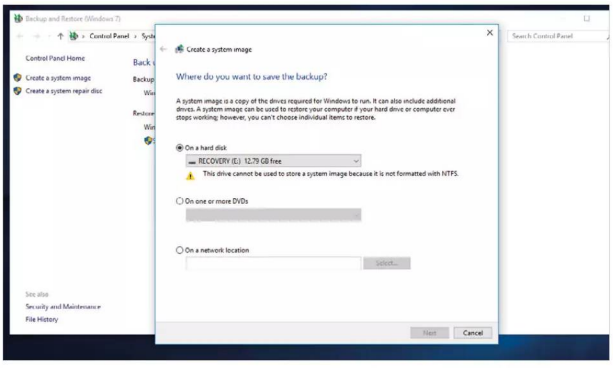
STEP 1 To begin, click on the Windows Start button and once more navigate to Settings > Update & Security > Backup. From within the Backup console window, where you were in the previous tutorial, click on the Go to Backup and Restore (Windows 7) link under the Looking for an older backup section.



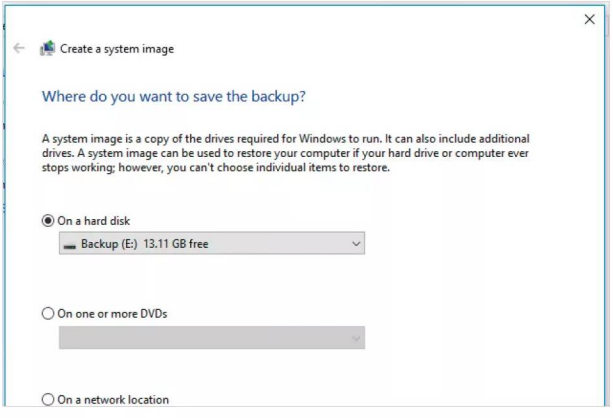
STEP 2 This will launch a new window, the Backup and Restore (Windows 7) console. Microsoft has kept this feature intact through Windows.1 and 10 purely due to compatibility support for backups done under older versions of the OS. To the left there are two links, click on the Create a system image link.



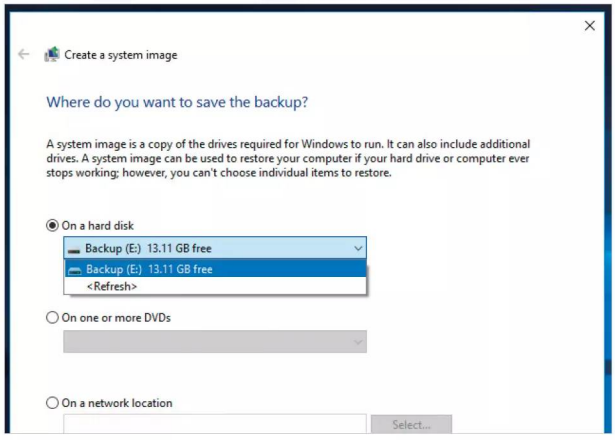
STEP 3 Windows will now scan your system for a drive that is able to house the system image files. You may need to make some changes to any drives according to what messages you get back from the scan. In this example, the drive we're using needs to be formatted as NTFS before Windows can use it.



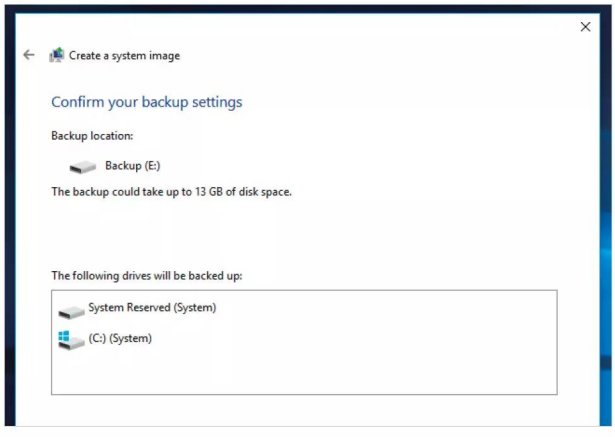
STEP 4 Providing you've met the requirements, you're offered a choice of where the system image can be written to. A drive is the quickest solution when it comes to restoring the image but you can opt for DVDs; it depends on the size of the image as to how many DVDs you need. You can even select a network location.



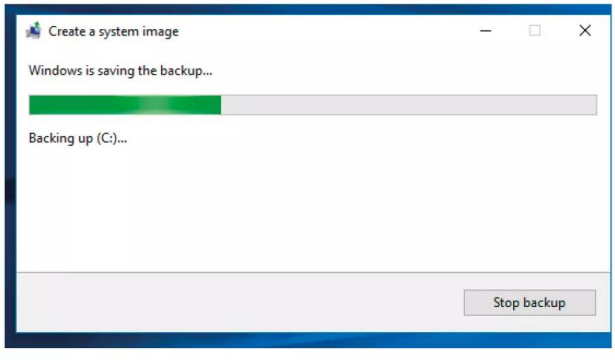
STEP 5 For this example, let's use an internal second hard drive. Make sure that the correct drive (it could be a high capacity USB stick or even portable USB hard drive) is selected, then click the Next button to continue.



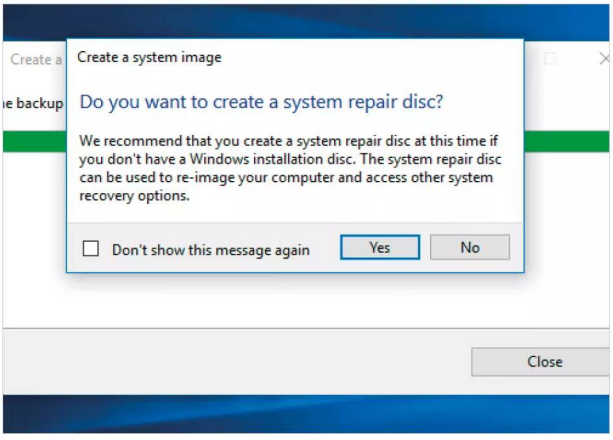
STEP 6 The next window will display the drives that are included in the system imaging process. In this example, the C:\ drive, the system drive and the System Reserved partition are to be backed up. When it comes to restoring the system you'll need both partitions for Windows to be able to boot up correctly.



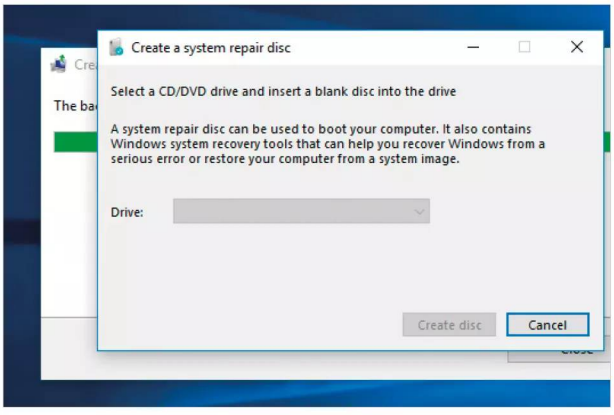
STEP 7 When you're ready to continue, click the Start Backup button. This will begin the imaging process, which can take some time depending on the amount of space used on the C:\ drive and the speed of the drive you're writing to. Allocate ample time if you're writing to DVD.



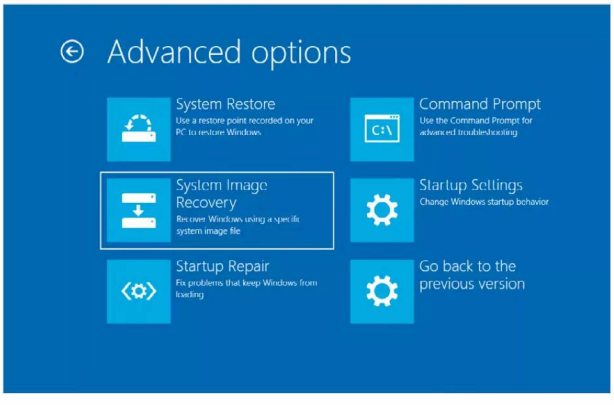
STEP 8 Once the process is complete, Windows will ask you to create a System Repair Disc. This disc will allow you to boot into the environment where you are able to launch the system image restore.



STEP 9 If you click Yes to creating the System Repair Disc you need to make sure you have a blank DVD to hand. Follow the on-screen instructions and click on the Create Disc button to burn the repair files to the disc.



STEP 10 Should you need to restore Windows from the system image, you can boot into the System Repair Disc and select the System Image Recovery option from within the Advanced Options of the Trouble Shoot menu. Follow the instructions and within minutes Windows will be back as it was when the system image was taken.



Extreme Windows Lockdown Tips

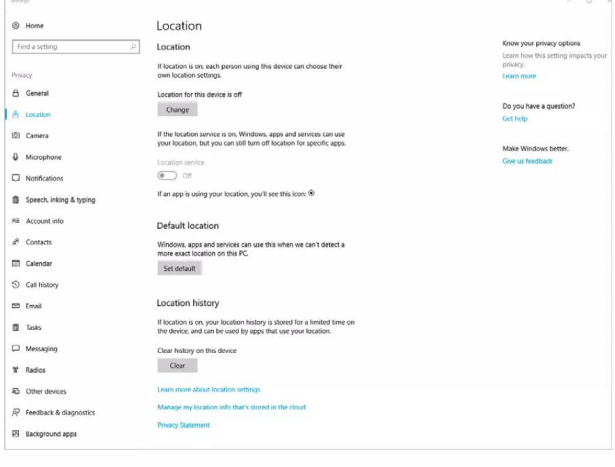
There are numerous ways and means to greatly improve Windows's security and privacy. Precisely how secure and private you want to get is purely down to you. You can opt for better than average or through these tips below, absolute extreme security.

Windows Security: The Paranoid's Guide

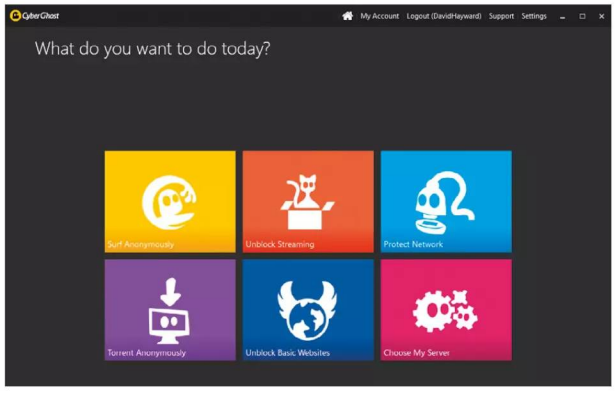
If you're fanatical about securing Windows and locking it down to the point where the NSA would be impressed, then follow these top ten extreme lockdown tips.

TIP 1 Let's begin with the easiest tip, unplug the computer from the Internet. Naturally there are disadvantages to this and you won't get updates for Windows or programs. However, you certainly won't get any Internet-borne malware infecting your machine.

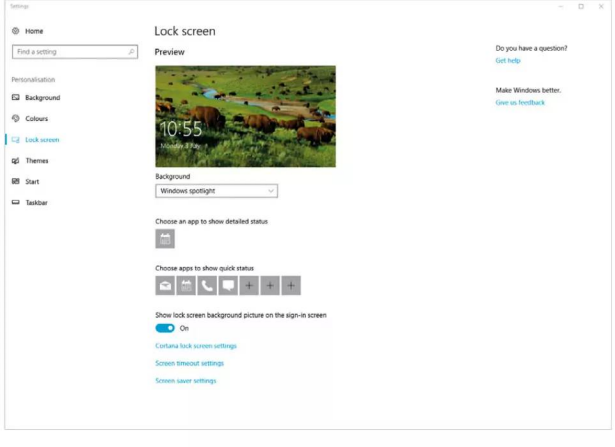
TIP 2 Click the Windows Start button and type privacy into the search box. Open the Privacy Settings link and turn off every option within the eighteen available Privacy sub-categories to the left of the console window.



TIP 3 When online use a VPN and where possible, also use the Tor browser. Both of these combined will greatly improve your anonymity and improve security by utilising the site blocking and anti-scamming properties of a good VPN such as CyberGhost.

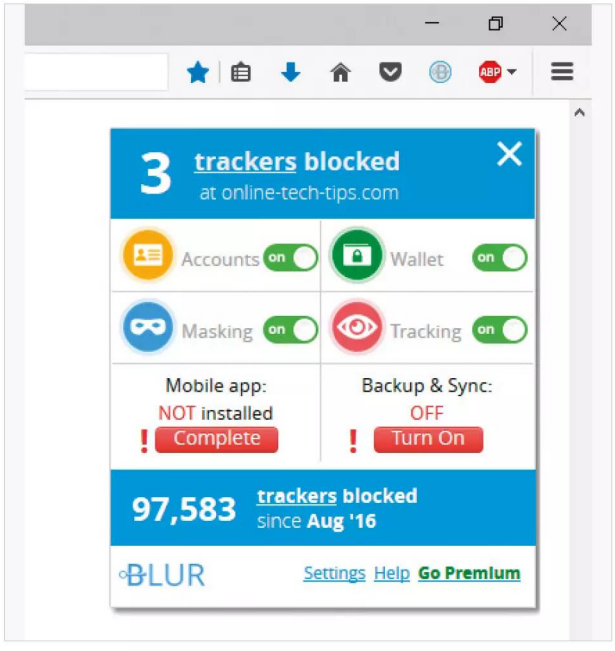


TIP 4 If you step away from your computer on regular intervals, you need to make sure that no one will be able to get on to it. From the Windows Start button type lock and click the Lock Screen Settings link. In here set a lock so that only you can get back to your desktop once you've entered a password.

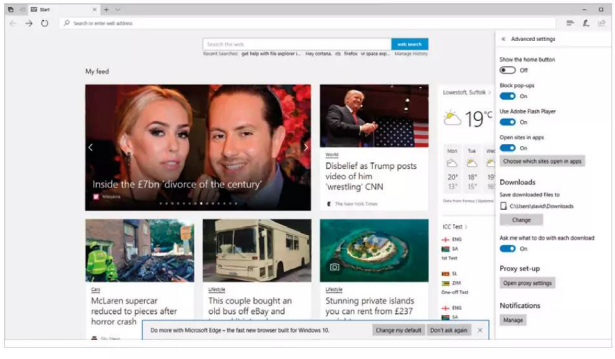


TIP 5 Depending on the age of your computer, it's possible to create a boot password from the BIOS. You need to consult your motherboard manual as to how to accomplish this but you can set a password for being able to boot into your computer (before Windows even starts) and getting into the BIOS itself.

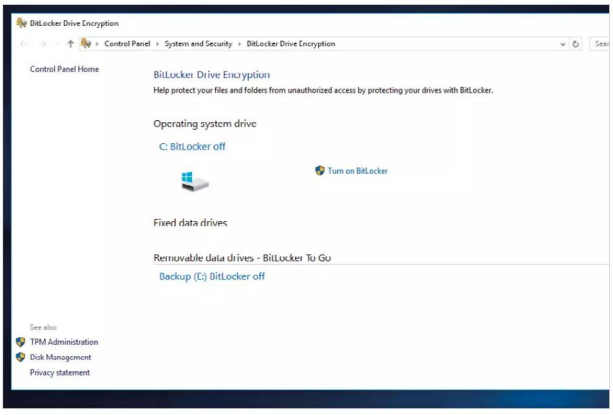
TIP 6 Consider installing several add-ons to your browser to improve its security and prevent any unwanted data miners or rogue scripts from being executed. Adblock Plus, Blur, No Script and other examples will secure your browsing session. For an extreme route, use the Tor browser.



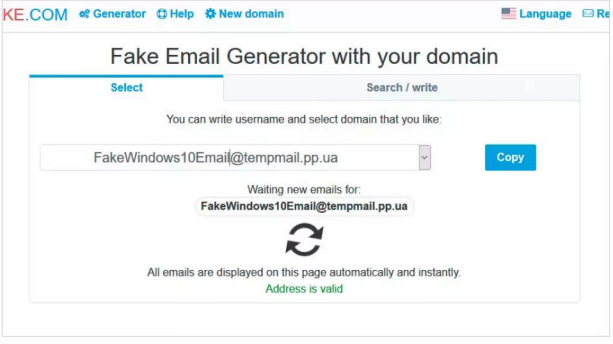
TIP 7 Flash and Java are superb entry points for malicious code to infect your computer and for snooping of various personal settings and data. Disabling both Java and Flash will prevent any such backdoors but limit your browsing experience on some sites.



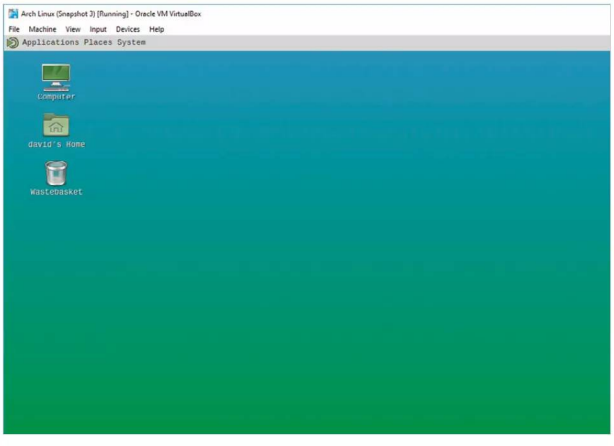
TIP 8 Encrypting your installed hard drives and any external devices you use is an excellent way of securing your data and locking down Windows. Whilst it can be inconvenient, you can be safe in the knowledge that any lost data is virtually unhackable by all but the military supercomputers.



TIP 9 Normally you'd use a valid email account to log into Windows, via an activated Microsoft account. However, consider setting up an alternative account that isn't linked to you. That way any data sent via Windows to other sources won't contain any personal data.



TIP 10 Use a Virtual Machine within Windows to conduct your day to day browsing and online work. The VM could be Windows too or even adopt a more secure environment such as one of the higher-end security versions of Linux. Either way, a VM will be far more secure than Windows on its own.

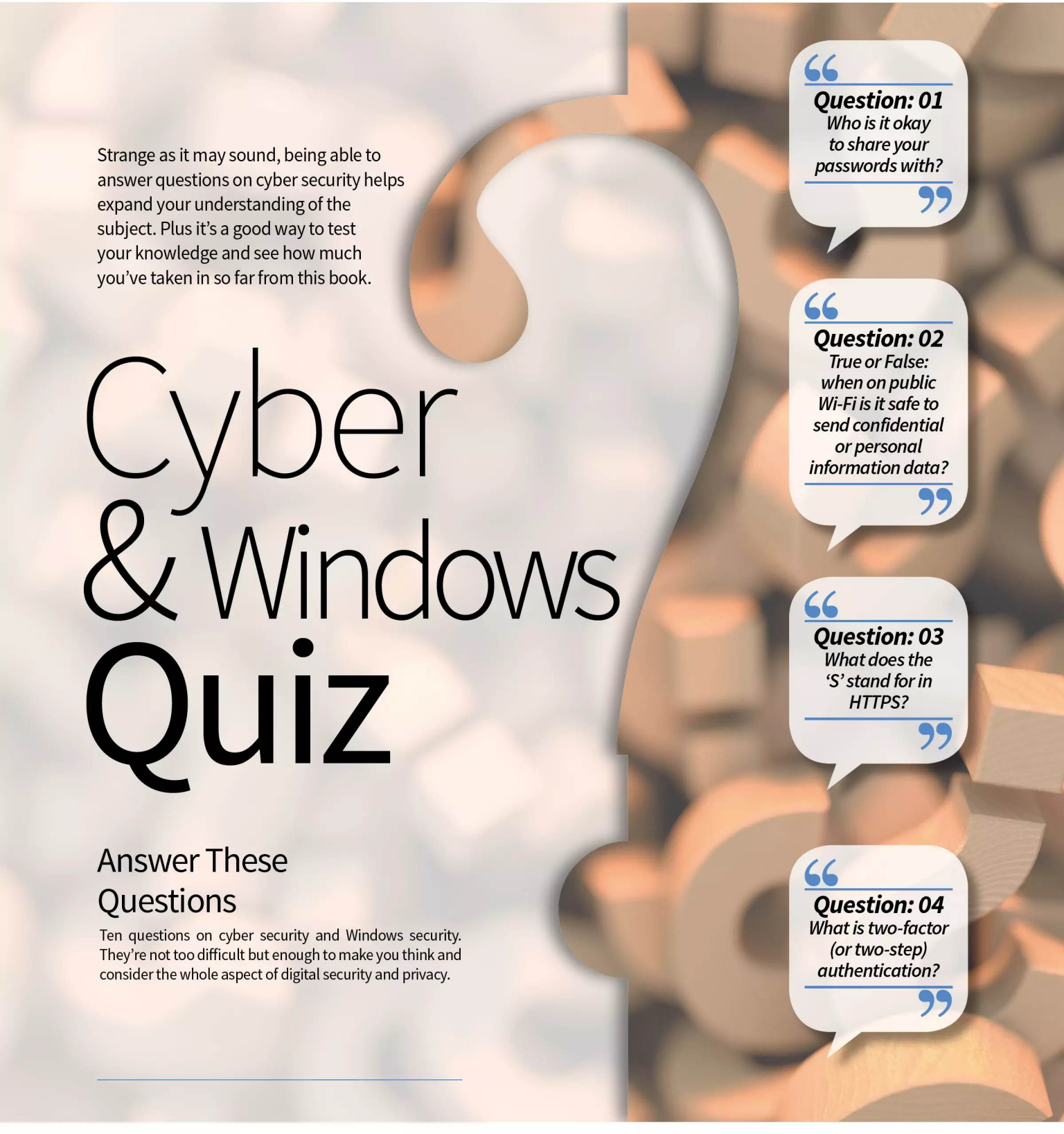


Strange as it may sound, being able to answer questions on cyber security helps expand your understanding of the subject. Plus it's a good way to test your knowledge and see how much you've taken in so far from this book.

Cyber & Windows Quiz

Answer These Questions

Ten questions on cyber security and Windows security. They're not too difficult but enough to make you think and consider the whole aspect of digital security and privacy.



Question: 05

Which of these is a Phishing attack?

- Sending someone an email that contains a malicious link disguised as a valid email.
- Creating a fake website that looks identical to a real one, in order to trick users into logging in.
- Sending someone a text message that contains a malicious link, disguised as something else.
- All of the above.

Question: 08

Which of these methods of browsing is the most secure?

- HTTPS
- Private browser mode
- VPN
- Tor

Question: 06

Which of the following passwords is the most secure?

- Password123
- ThV%100*Vx!
- LetM31N
- 123456

Question: 09

What does AES stand for?

Question: 07

Give five examples of malware

Question: 10

How often should you review your Windows security and updates?

- Once a month
- Once a day
- Once a week
- Once only, just after installation of Windows

Answers:

1 No one. Never tell anyone your passwords.

2 False. Never send personal or confidential data when using public Wi-Fi

3 Secure, meaning it's encrypted. Hyper Text Transfer Protocol Secure.

4 A multi-step authentication method requiring username and password, as well as extra information. Usually via a text message.

5 All of the above. All are forms of Phishing.

6 ThV%100*Vx!. It contains multiple characters, caps, lower case and isn't a dictionary word.

7 Ransomware, Virus, Adware, Trojan Horses, Worms.

8 VPN. Tor is very secure but is subject to vulnerabilities.

9 Advanced Encryption Standard.

10 Once a day. You should look at your Windows security at least once every day.

What the Experts Say

Amongst the many quotes from security experts of the modern digital age, some stand out as either remarkably fortuitous or simply worth mentioning. We've compiled ten top quotes from the security world, that both entertain and make you think.

> *Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds*

> If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.

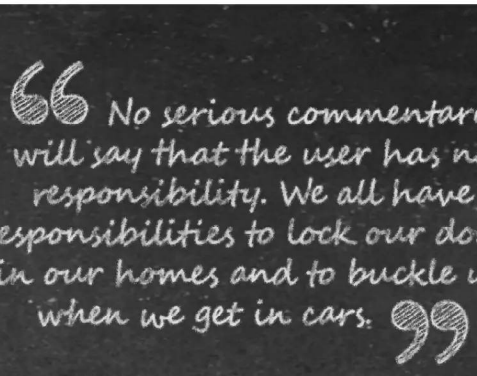
White House Cybersecurity Advisor, Richard Clarke.

> Computer security can simply be protecting your equipment and files from disgruntled employees, spies and anything that goes bump in the night, but there is much more. Computer security makes sure no damage is done to your data and that no one is able to read it unless you want them to.

Bruce Schneier, Protect Your Macintosh, 1994.

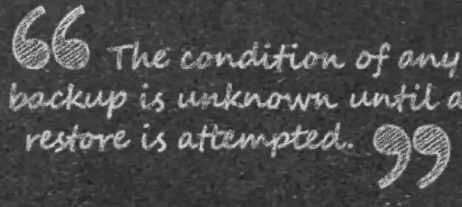
> The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.

Gene Spafford.



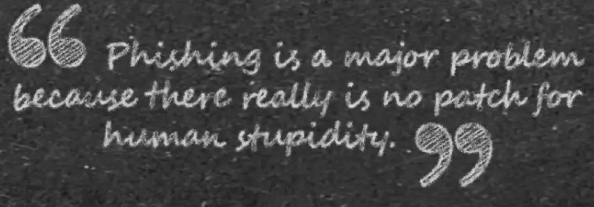
> No serious commentary will say that the user has no responsibility. We all have responsibilities to lock our doors in our homes and to buckle up when we get in cars.

Spokesman, Information Technology Association of America, Business Roundtable, AP, May 19, 2004.



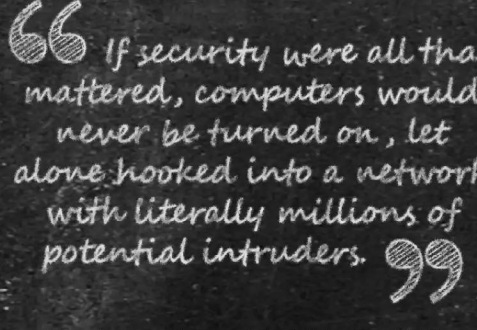
> The condition of any backup is unknown until a restore is attempted.

Schrodinger's Backup.



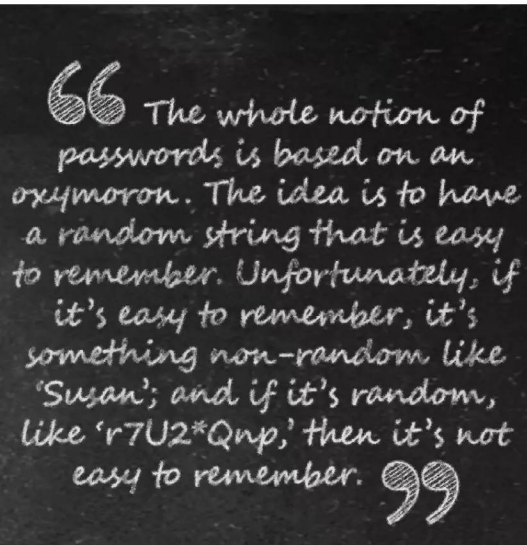
> Phishing is a major problem because there really is no patch for human stupidity.

Mike Danseglio, program manager in the Security Solutions group at Microsoft, April 4, 2006.



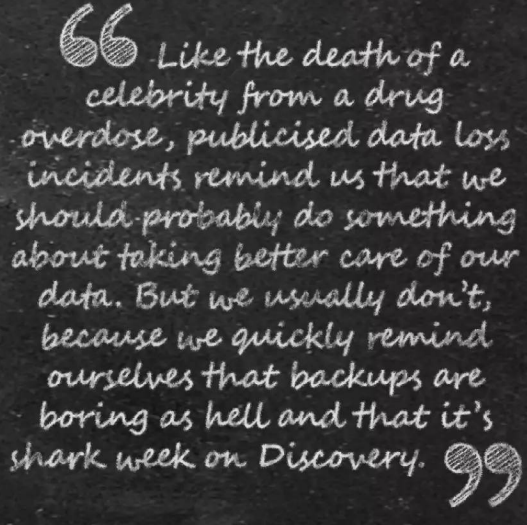
> If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders.

Dan Farmer, System Administrators Guide to Cracking.



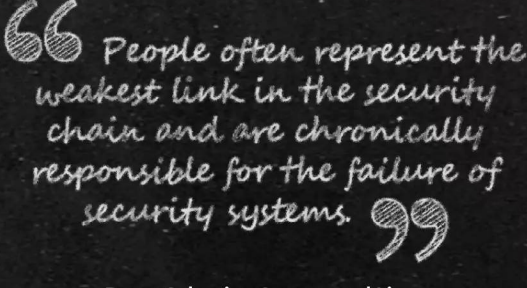
> The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it's easy to remember, it's something non-random like 'Susan'; and if it's random, like 'r7U2*Qnp,' then it's not easy to remember.

Bruce Schneier.



> Like the death of a celebrity from a drug overdose, publicised data loss incidents remind us that we should probably do something about taking better care of our data. But we usually don't, because we quickly remind ourselves that backups are boring as hell and that it's shark week on Discovery.

Nik Cubrilovic, TechCrunch.com, October 10, 2008.



> People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.

Bruce Schneier, Secrets and Lies.

Home Networking Tricks & Tips
6 | ISBN: 978-1-912847-56-3

Published by: Papercut Limited
Digital distribution by: Readly AB

Papercut Limited
Registered in England & Wales No: 04308513

ADVERTISING - For our latest media packs please contact:
Brad Francis - brad@papercutltd.co.uk
Web - www.pclpublications.com

INTERNATIONAL LICENSING - Papercut Limited has many great publications and all are available for licensing worldwide.
For more information email: jgale@pclpublications.com