techgo

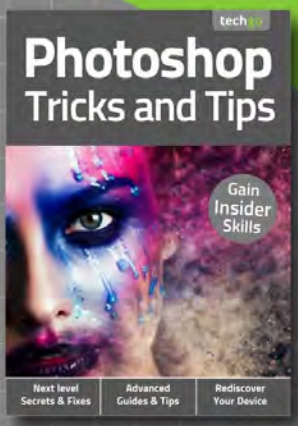
Online Security Tricks and Tips

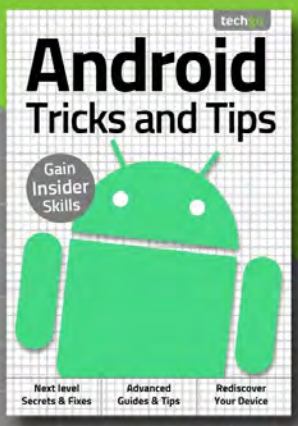
Next level Secrets & Fixes

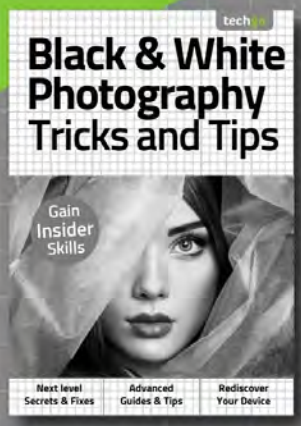
Advanced Guides & Tips

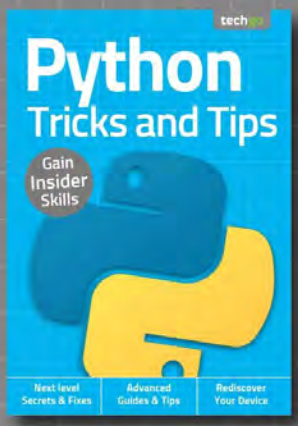
Rediscover Your Device

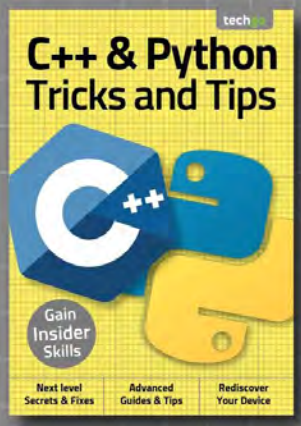
Discover more of our guides...

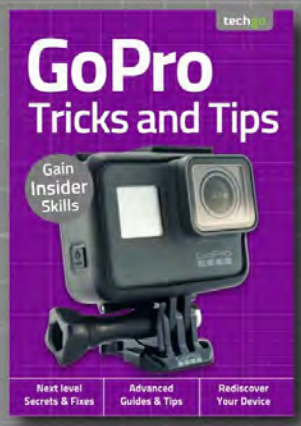


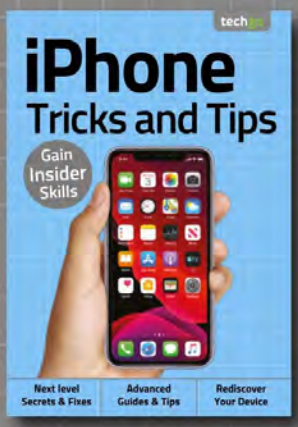


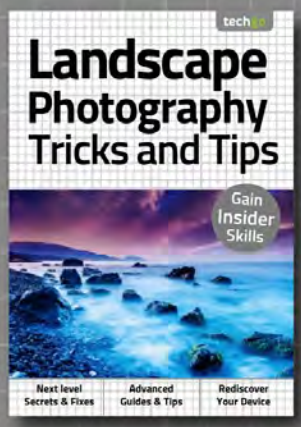












techgo

Online Security For Beginners

Welcome back... Having completed our exclusive For Beginners digital guidebook, we have taught you all you need to master the basics of your new device, software or hobby.
Yet that's just the start!

Advancing your skill set is the goal of all users of consumer technology and our team of long term industry experts will help you achieve exactly that. Over this extensive series of titles we will be looking in greater depth at how you make the absolute most from the latest consumer electronics, software, hobbies and trends!
We will guide you step-by-step through using all the advanced aspects of the technology that you may have been previously apprehensive at attempting. Let our expert guide help you build your understanding of technology and gain the skills to take you from a confident user to an experienced expert.

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

6 Advanced Security Tips

8 Windows 10 Privacy Settings
10 How to Check which Apps are Sending Information
12 What is a firewall?
14 Improving the Windows 10 Firewall
16 Creating a Security Plan
18 Windows Security Checklist
20 What is a Sandbox?
22 Running Windows 10 as a Sandbox
24 Installing VirtualBox
26 Installing Windows 10 in VirtualBox
28 Creating VirtualBox Snapshots of Windows 10
30 Create a Windows 10 Recovery Drive
32 How to Back Up Windows 10
34 How to Create a Windows 10 System Image
36 Extreme Windows 10 Lockdown Tips
38 Cyber and Windows Quiz
40 What the Experts Say

42 Online Child Protection

44 Children Online: What are the Risks?
46 Social Media & Children
48 Search Engine Safety
50 Online Grooming
52 How Safe are the Sites Your Child Can Access?
54 Email and Child Safety
56 Top Child Friendly Email Programs and Services
58 Cyberbullying
60 How to Prevent and Deal with Cyberbullying
62 Helping Your Child Through the Internet
64 Your Child and Online Gaming, is it Safe?
66 Staying Safe when Gaming Online – Advice for Your Child
68 Monitoring What's Going On
70 Monitoring Online Activity for Non-Technical Guardians
72 Tips for Technical Guardians to Monitor a Child's Online Activity
74 Ten Monitoring Tools to Install and Use
76 Using the Windows Hosts File to Block Sites

78 Further Protection for Young Adults

80 Staying Safe with Facebook for Teens
82 Staying Safe with Twitter for Teens
84 Staying Safe with Instagram for Teens
86 Staying Safe with WhatsApp for Teens
88 Staying Safe with Snapchat for Teens
90 Creating a Child Account in Windows 10
92 Windows 10 Family Features
94 Problems with In-app Spending
96 Tips on How to Stop In-app Overspending
98 Online Child Safety at School
100 Where to Find Help with Online Child Safety
102 What the Experts Say
104 Glossary of Terms

"...we cover advanced security methods and also looking out for your children when online, together with guides on how best to protect them. You'll soon be security savvy and prepared for whatever digital threat looms on the horizon..."

Online Security Tricks and Tips
2nd Edition
ISBN: 978-1-912847-66-2
Published by: Papercut Limited
Digital distribution by:
Readly AB, Zinio, Magzter, Cafeyn, PocketMags

Papercut Limited
Registered in England & Wales No: 4308513

@bdmpubs BDM Publications www.bdmpublications.com

Advanced Security Tips

If you want to improve your Windows security further, then this section looks 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 10 and all your data, so should something happen you'll be able to restore your files with confidence.

Windows 10 Privacy Settings

Windows 10'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 10 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 10 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 10 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 10, 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 10 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 10 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 10 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 10 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 10'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 10 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.

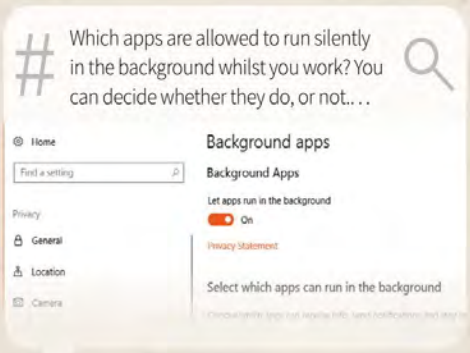
Microphone – The same applies for the computer's microphone; which apps can access it or not, and whether you want to globally turn it off.

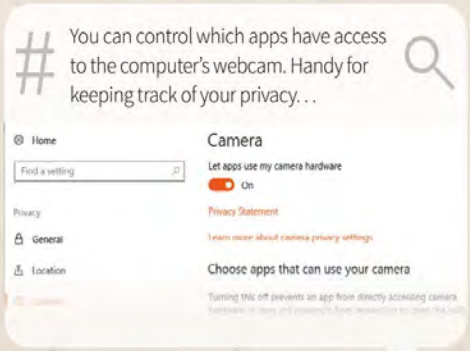
Contacts – The Contacts section details which apps can have access to your current Windows account contacts. Disabling this globally may have a severe impact on how some apps, such as Skype and email work.

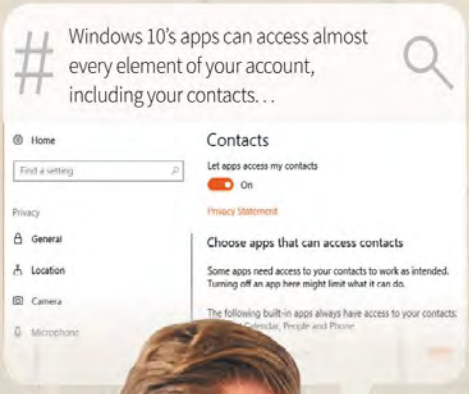
Radios – This option will define which apps can control hardware such as the computer's Bluetooth device, Wi-Fi or any other kind of wireless receiver. Obviously, some apps will require access to share information or allow access to shared areas.

Background Apps – Windows 10'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 10 user should do. This way you become familiar with how the OS shares your account data and what exactly has access to your Windows 10 computer and its hardware.







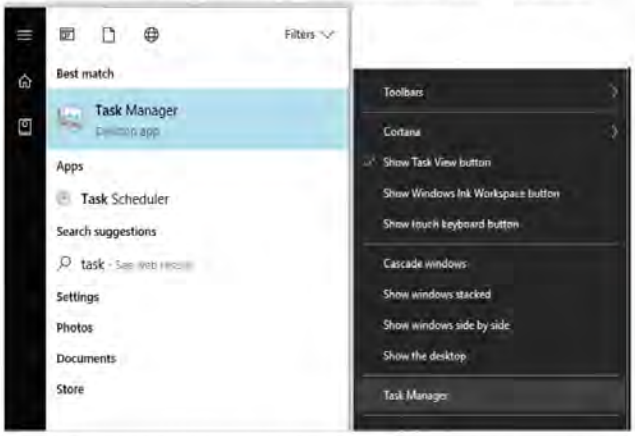
How to Check which Apps are Sending Information

Most Windows 10 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.

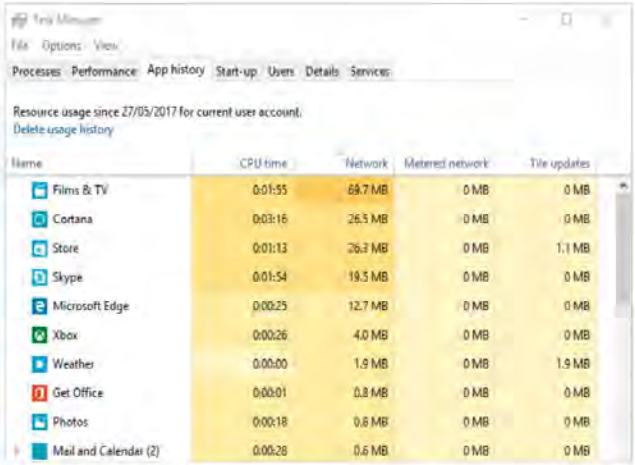
Look Who's Talking

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.

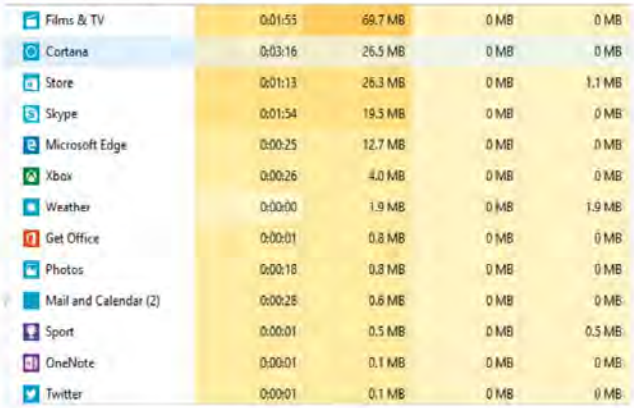
STEP 1 The first port of call to help monitor what apps are accessing the Internet is Task Manager. Click the Windows Start button and type task, then click the Task Manager result in the search box. You can also right-click the taskbar and select Task Manager from the available option in the menu.



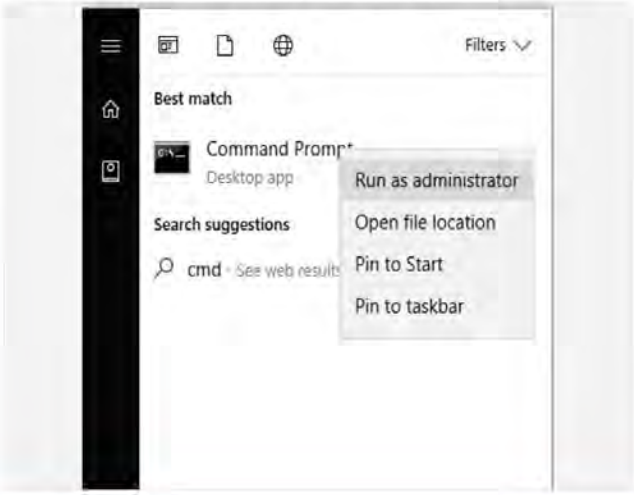
STEP 2 With Task Manager displayed, click the More Details arrow (if it's available). This will expand the Task Manager options. From here, click the App History tab and then the Network column so that there's a downward pointing arrow above it. This indicates network use in a descending order of amount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



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.



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.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -e -s -p tcp -b
Interface Statistics

                           Received            Sent

Bytes                     596867720        65196200
Unicast packets              515780          349675
Non-unicast packets           16485            6265
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

TCP Statistics for IPv4

  Active Opens                            = 5067
  Passive Opens                           = 405
  Failed Connection Attempts              = 121
  Reset Connections                       = 763
  Current Connections                     = 16
  Segments Received                       = 712631
  Segments Sent                           = 572026
  Segments Retransmitted                  = 7899
```

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.

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:55247        Windows:65001          ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:55366        Windows:55387          ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:55387        Windows:55366          ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:55407        Windows:55408          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55408        Windows:55407          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55414        Windows:55415          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55415        Windows:55414          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55416        Windows:55417          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55417        Windows:55416          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:65001        Windows:55247          ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.180:55255    db5sch101101426:https  ESTABLISHED
```

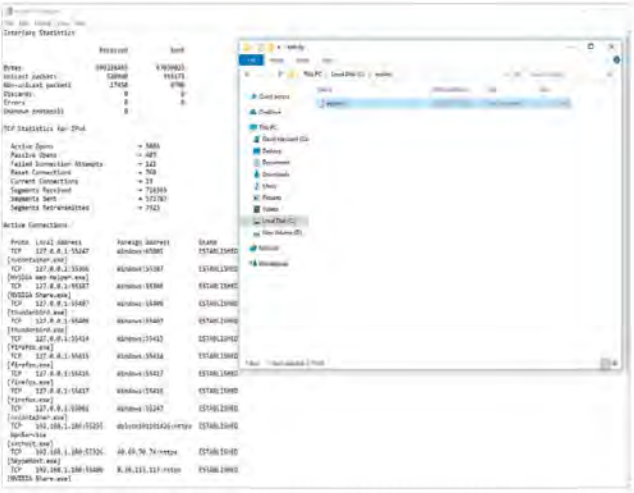
STEP 7 If you want to create a friendlier way of viewing Netstat active connection data, you can pipe the contents to a text file. For example, in the command prompt enter **cd** to take you to the root of the C: drive. Then create a new folder to store the text file with **md activity**, and enter it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

```
Administrator: Command Prompt

C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\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.

```
Administrator: Command Prompt

C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\activity>netstat -e -s -p tcp -b > activity1.txt

C:\activity>
```

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.

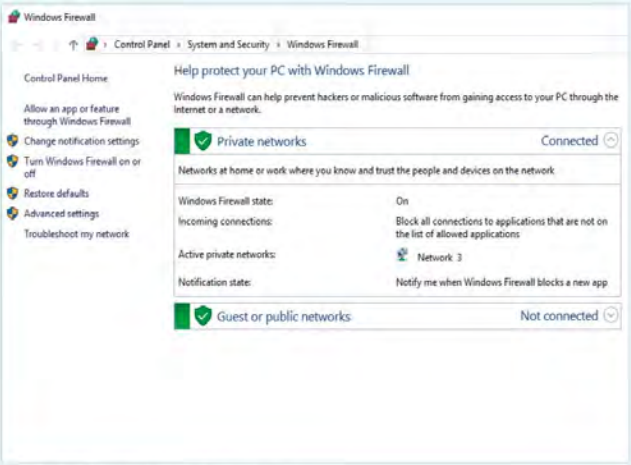
In its simplest guise, a firewall will look to a defined set of rules then apply those rules to any data packets that pass through it. For example, if you've created a rule whereby all Telnet traffic is blocked, any packet that's trying to reach port 23, the port that Telnet applications listen on for 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.

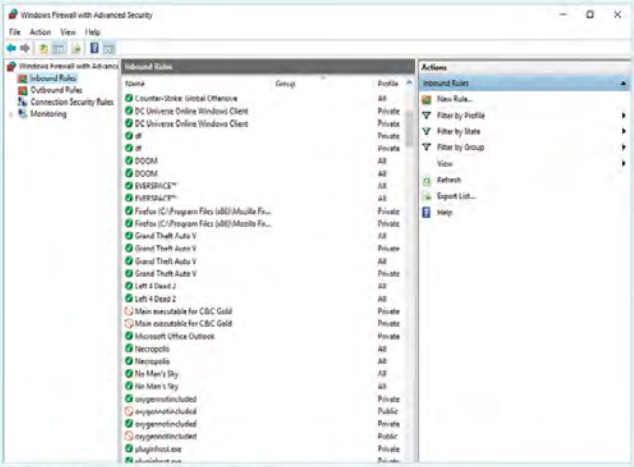
A further layer of protection was included into the basic firewall early in the 2000s. Application-layer analysis enabled firewalls to inspect packets that were targeting individual applications within the operating system. Each program or application installed in the system will use a set of protocols to communicate with the outside world. When an application is installed, on a Windows 10 system for example, the installation mechanism will automatically add an instance of it to the Windows 10 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 10 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 10 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."

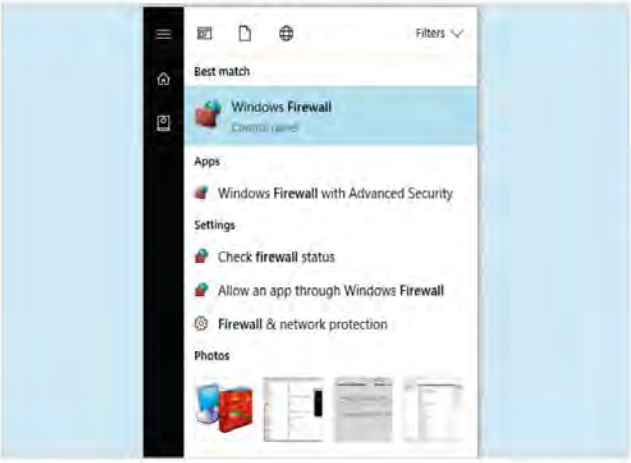
Improving the Windows 10 Firewall

The built-in Windows 10 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.

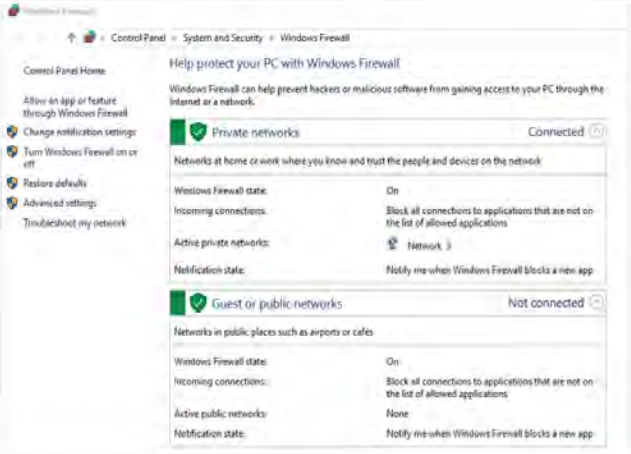
Getting to Know Your Firewall

Generally, there's little need to ever configure the Windows 10 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 10 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.

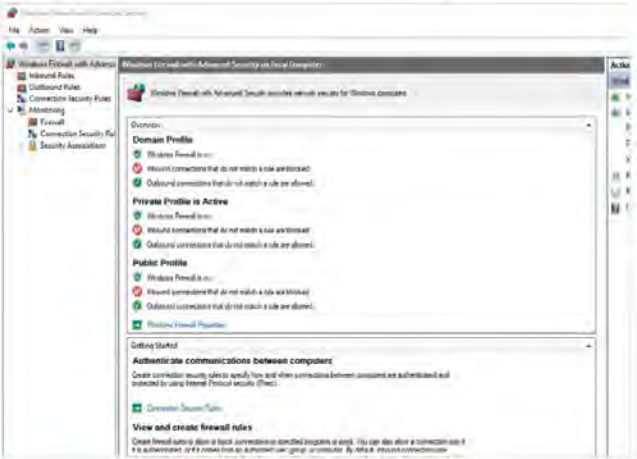


STEP 2 The Windows 10 firewall console window starts by detailing the basic status of the firewall. It should be On by default, unless you've installed a third-party security suite which contains its own firewall. There are two kinds of network listed, Private and Public. Private is for home or work, whereas Public is for cafés and the like.



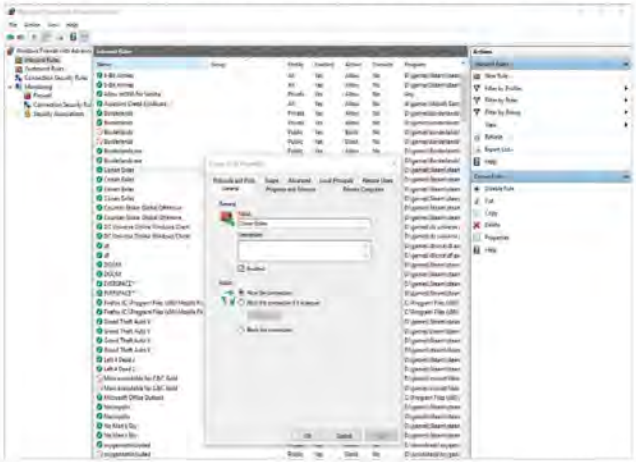
STEP 3 Down the left-hand side are some links that will help you configure and improve the firewall, as well as turning it on or off (which isn't recommended under any circumstance other than the installation of an improved third-party firewall). To begin with, start by clicking on the Advanced Settings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

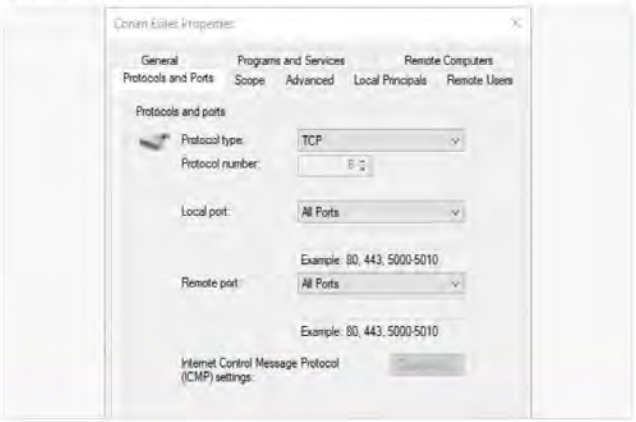


STEP 5 Click on Inbound Rules to the right-hand side of the main console window. This will list the current rules that allow traffic into your computer and to the applications that require it. For example, in this screenshot there are rules for various games that allow multiplayer interaction and the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

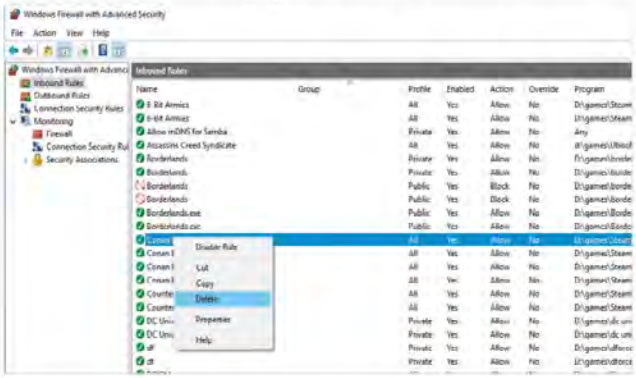
STEP 6 These rules are automatically entered into the firewall when you install the program, game or app. When you install a program you're required to accept and authenticate the process, clicking on Yes to start the installation. This level of administrative access also allows entry of the program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



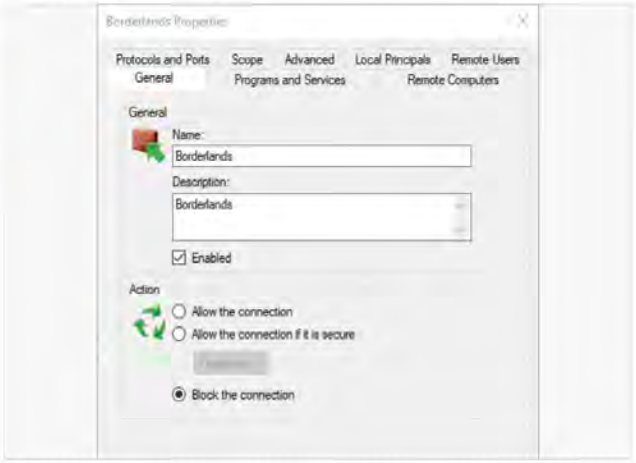
STEP 7 The properties of each firewall entry allow a greater degree of control for that particular program. You can change the name of the entry, allow or block the connection, define the physical location of the program on your computer, allow access to the program from remote computers, set the protocol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



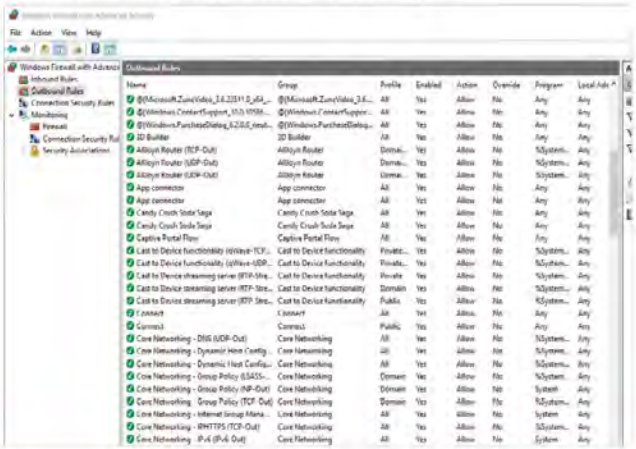
STEP 8 Sometimes, uninstalling a program doesn't automatically remove it from the Windows firewall. The exact reasons why are varied but to help improve the efficiency of the Windows firewall, whenever you remove a program from your system, it's worth checking the firewall to see if its entry has been 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

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.

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

Updates

Obviously a must-have section of a good security plan is to regularly check for system and program updates. Thankfully, Windows 10 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.

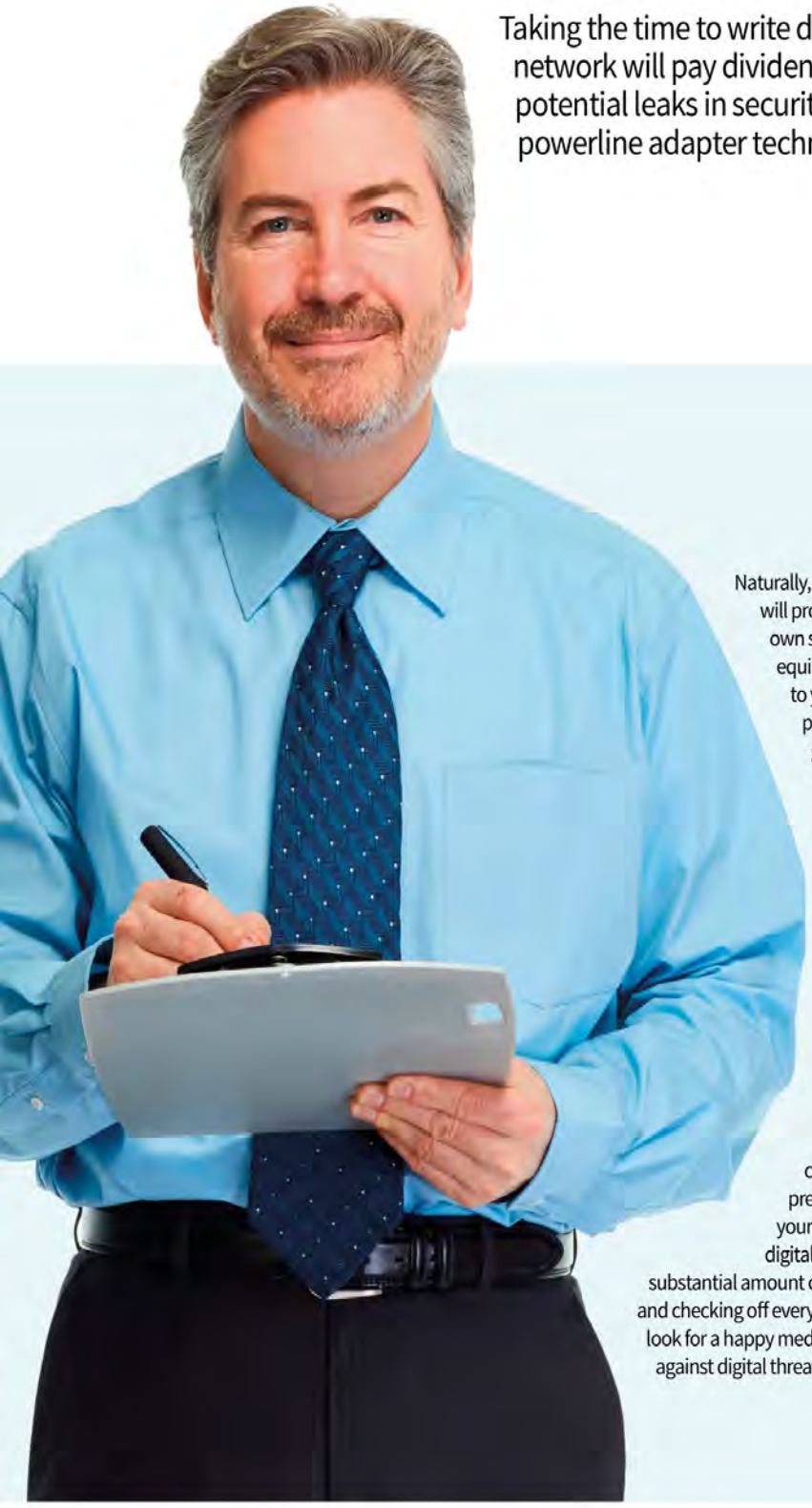
Cabling

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 10 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.

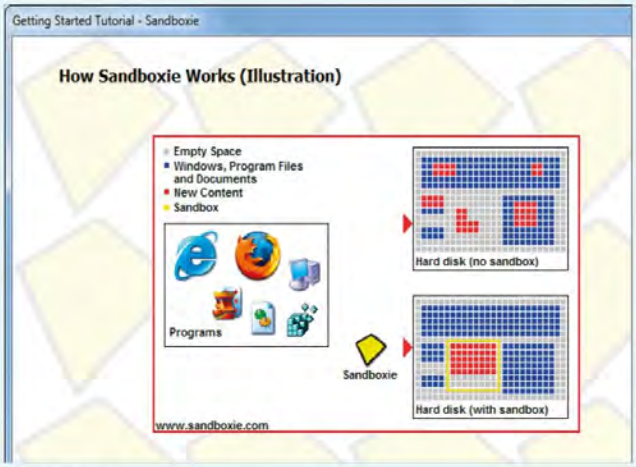
It's not always the testing of malicious code that's associated with sandboxes. For example, the words you're reading now were written using Office 365/Word 2016. Before the product was released by Microsoft, the development team behind Word will have gone through extensive testing, making sure that 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 10 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 10 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 10 sandbox is beneficial to the average user.

OLD PROGRAMS

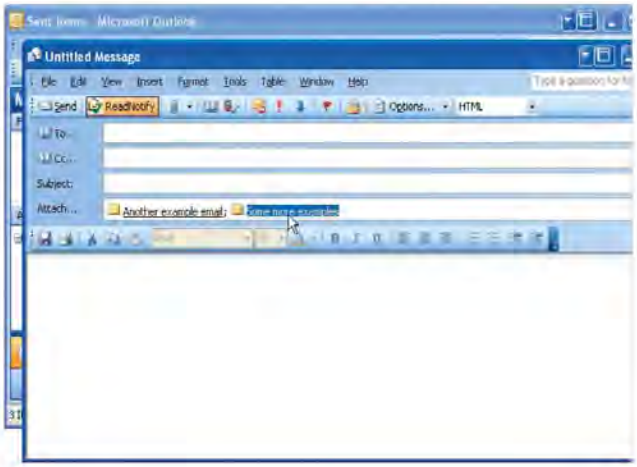
Within the Windows 10 virtual sandbox environment you may be able to run older programs that would normally fail, even in compatibility mode, under more modern hardware drivers. Often an older program will look for a specific driver set, if it's too modern then it can fail. Virtual environments use older 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.

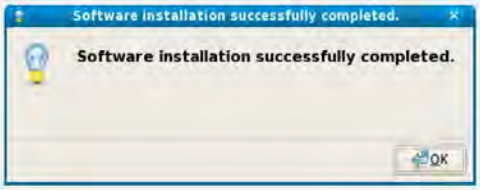
HOST PROTECTION

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 10 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 10 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 10 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