Home Networking For Beginners

Get started with networking & smart devices

100% INDEPENDENT

Papercut

Home Networking For Beginners

Home Networking For Beginners is the first and only choice if you are a new adopter and want to learn everything you'll need to get started with the your home network hub. This essential manual is crammed with helpful guides and step-by-step fully illustrated tutorials, written in plain easy to follow English. Over the pages of this new user guide you will clearly learn all you need to know about the home networking. With this unofficial instruction manual at your side no problem will be unsolvable, no question unanswered as you learn, explore and enhance your networking skills.

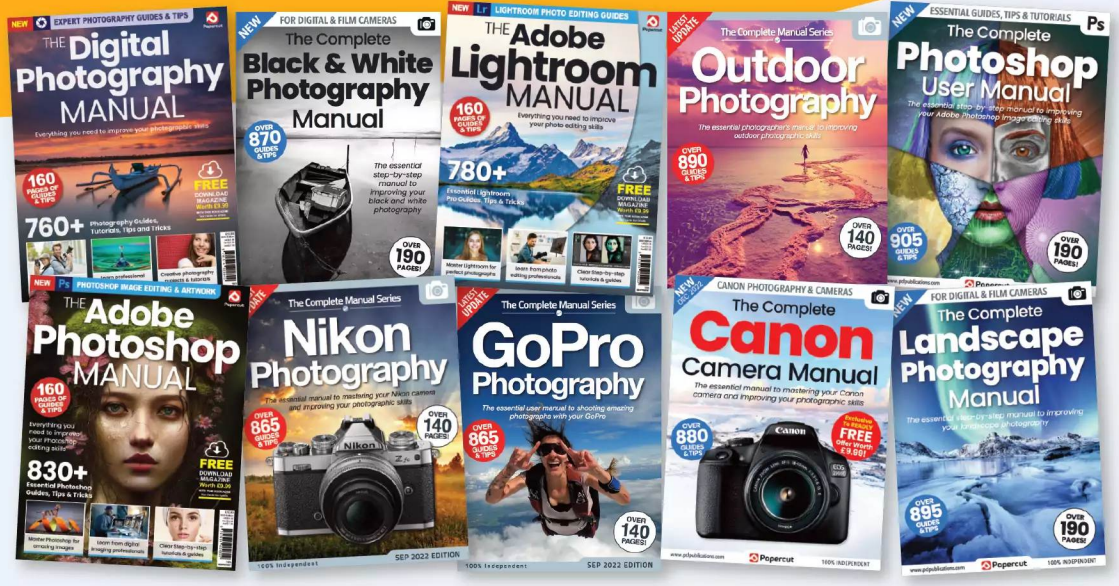
Papercut

www.pclpublications.com

Save a whopping 25% Off!

Photography & Photoshop Manuals

with Papercut



Not only can you learn new skills and master your camera, but you can now SAVE 25% off all of our photography, Photoshop and tech digital and print manuals!

Simply use the following exclusive code at checkout:

NYHF23CN

www.pclpublications.com

Get Your Exclusive FREE Gift Worth £9.99 Here!

Download Your FREE Copy of Tech Shopper Magazine

Head over to your web browser and follow these simple instructions...

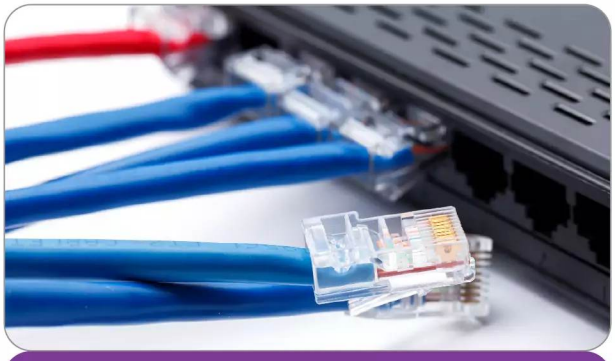
1/ Enter the following URL: **www.pclpublications.com/exclusives**
2/ Sign up/in and from the listings of our exclusive customer downloads, highlight the Tech Shopper Magazine option.
3/ Enter your unique download code (Listed below) in the "Enter download code" bar.
4/ Click the Download Now! Button and your file will automatically download.
5/ Your file is a high resolution PDF file, which is compatible with the majority of customer devices/platforms.

Exclusive Download Code: PCL37862RE

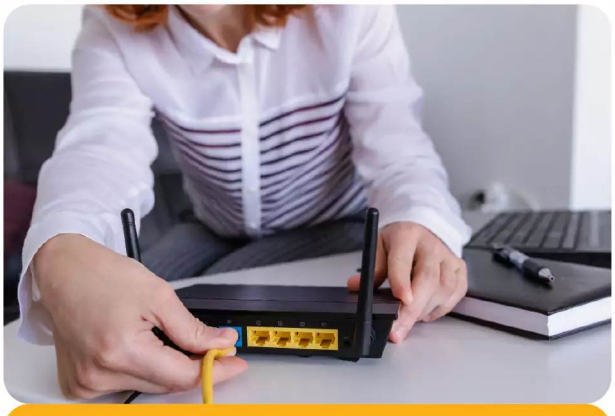
NOTE: This is a limited reader offer running from 1st March to 1st July 2024.
Terms and conditions apply and can be found at www.pclpublications.com

Contents

HOME NETWORKING



42 Networking Home Entertainment



54 Combat Network Issues

64 How To Protect Yourself

Introduction To Home Networking

The home network can be as simple as a single router and computer, browsing the Internet and watching the occasional episode on Netflix and the like. However, most of us have far more complex setups, and we don't even realise it.

Along with a smart TV, there's usually a number of tablets, phones, laptops, computers, games consoles, AI devices such as Google Home and so on. Plus any number of security cameras, baby monitors, remote doorbells; the list of connected devices goes on.

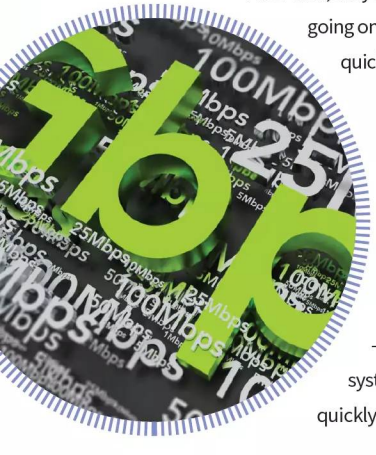
We've increased the number of devices on our networks, but what do all these pieces of networking equipment do, and how to do they work? You'll find out in this chapter.

Your Home Network

Your home network is something most of us don't even consider when we power on our devices and computers and surf the Internet; however, there's more to it than you think. How do we get on the Internet? How do we print from all our devices? How does it all work? Let's have a look.

Consider the average user: they contact an Internet Service Provider (ISP), sign up for a broadband deal, and in a day or two they receive their router through the post. This they hook up to their existing telephone line, power up, then wait as the lights on the router turn a certain colour indicating that a connection is made. They can then turn on their computer or device, locate the Service Set Identifier (SSID, the router's name), enter the wireless password and connect to the Internet.

After that, they tend to forget all about the router and what's going on. Unless there's a problem, then usually a quick reboot of the router will solve the issue.



There is a lot more going on in the background though, and if you take the time to learn a little about how networking works, then you'll discover that you're able to get more out of your network. This includes better speeds, more capability – such as setting up a home entertainment system, better security, and you'll be able to quickly diagnose any problems should they ever arise. In short, creating and maintaining a good home network will make your digital and online life significantly better in the long run.

Getting the most from your network

While you may think your network is running perfectly fine, there are undoubtedly areas of improvement. These areas include surfing the Internet, online gaming, watching streaming video services, watching content on multiple devices around the home, being able to get access to your network from the extremities of your home or garden, and more. All these elements can be enhanced on, it's just knowing what to tweak and how to get the most from what you have available.

Before we begin to look at how to improve your network, it's worth noting that you do have a physical limit on what you can achieve. There's only so much bandwidth available to your home from your ISP, so while you can streamline your access to the Internet, you're not going to be able to increase that limit. Likewise, the data that moves around your home will also hit a physical limit. Most wireless devices will find the fastest possible connection to your router, and wired devices (using an Ethernet cable), and computers will communicate at either 100Mb/s or 1000Mb/s (or 1Gb/s). It's possible to improve the connection, but not increase the limits of the actual hardware. A good rule of thumb to always remember when networking, either on a home network, office networks or the entire Internet, is that the connection speed is only as fast as the slowest component on the network.

Of Bits and Bytes

Megabytes and megabits are two of the most commonly misused terms in computing talk. Both are measured units of computer data, but in terms of the capacities of hard drives and the amount of memory in our PCs we are referring to bytes; whereas in terms of the speed of our network, or Internet access, then we are talking about bits.

Basically, there are 8 bits to a byte, and a million of these bytes make up a megabyte, or 1 MB, which is used when we talk about hard drive storage or an amount of memory. Furthermore, a thousand megabytes (1000 MB), is 1 GB, or gigabyte and a thousand gigabytes makes a terabyte (1 TB). So when we say 'that hard drive has a huge capacity of 3TB', we mean it can hold three thousand gigabytes, or three million megabytes.

More accurately speaking however, there are actually 1024 bytes in a kilobyte and 1,048,576 (1024 x 1024), bytes in a megabyte (1 MB, again).

Hard drive manufacturers these days generally only refer to the single unit equivalent of GB or TB. With that in mind, it's interesting to note that the example we used earlier, of 3TB (three terabytes), is really 3,145,728 megabytes or 3072 gigabytes. So as you can see, using the simplified version makes life a little easier; although the purist may disagree.

Megabits, when we talk about data transfer rates, the speed of your Internet connection and so on are represented as Mb; note the lower case 'b'. To make things a little easier, in the world of telecommunications the Mb equals 1,000,000 bits. So 1 Mbps, which is a single megabit per second, is the same as 1,000,000 bits per second.

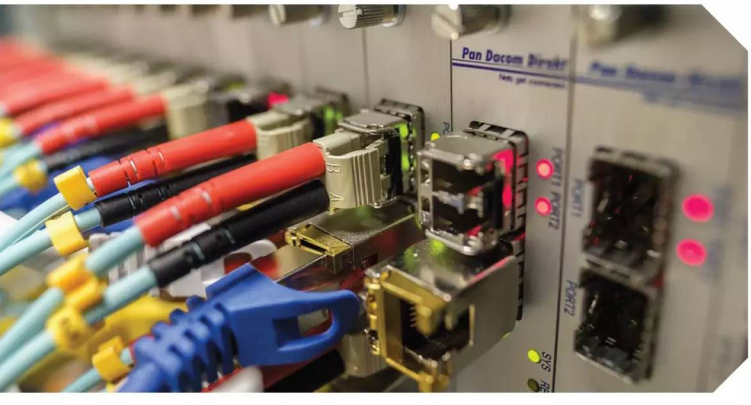
If you use the common byte size of 8 bits, then 1 Mb (megabit), is roughly equal to 0.125 MB (megabytes). So, if you're not foaming at the mouth by now, a decent broadband line advertised at 75 Mbps can transfer data to your PC at around 9.375 MB/sec (megabytes per second). And, your home network with a 100 Mbps switch will send data from one PC to another at around 12.5 MB/sec, whereas with a gigabit Ethernet switch and network ports on the PC, will transfer the data to and from one computer to the next at around 125 MB/sec.

As we said, these are only theoretical speeds, even those advertised by your ISP. In theory you can reach these speeds, but external factors such as cable quality, noise on the line and so on can have an affect on the total overall performance of the line.

Either way, we can still improve what we have, and ensure that our network is in as tip top shape as possible. If it's working well, then you'll have no complaints from the other members of the family.

Routers: How do they work?

Every Internet connected home, office, and multi-site megacorporation in the world uses a router to connect to the Internet. The router is the bridge that gaps your home network to the wider world of the Internet, as well as being the hub of all your connected devices.



A router is simply a piece of hardware that's designed to interconnect one network to another. They can be used to connect two individual office networks together, so the teams in each can share resources, but more specifically, in terms of the home user, they're used to connect all your devices to each other and ultimately the Internet.

Routers come in various shapes and sizes, offering many features; with some of the higher-end models offering more. Typically, a router, the one you'll receive from your ISP when you sign up to a broadband deal, will be able to do the following:

- Connect to the Internet
- Assign individual IP addresses to connected devices
- Form a layer of security to protect your home network
- Offer wireless connectivity to devices
- Have a built-in switch for multiple devices via Ethernet cables
- Network Address Translation (NAT)
- Resource sharing
- Parental or safety controls
- Port forwarding
- Upgradable Firmware.

So what do all these mean?

Connect to the Internet

Your router will function as a bridge between your computer and the Internet via the ISP's network. What this means is, your ISP has sent you a device that's configured to access their network, so when you connect it at home, it will begin to transmit and receive data to and from your computer and the ISP. The ISP itself will have its own connection to the Internet, a very big one, and will share that bandwidth out with all its customers. With you being a customer, you'll get a share of bandwidth equal to the broadband package you're paying for.

Assign Individual IP Addresses to Connected Devices

One of the router's primary functions is to allocate IP addresses. An IP address is a unique network identifier that allows communication across the network; every computer connected to the Internet has a unique IP address. These addresses work in much the same way as a postal address; they contain the information needed to get to where they're going and where to return.

There are two types of IP address, the first is IPv4: IPv4 uses 32 binary bits to create a single address on the network. An IPv4 address is expressed

by four numbers separated by dots. Each number is the decimal representation for an eight-digit binary number; also called an octet. For example: 192.168.1.150
IPv6 uses 128 binary bits to create a single unique address on the network. An IPv6 address is expressed by eight groups of hexadecimal numbers separated by colons, as in 2a00:23c7:c87:d101:e8a1:c3d7:ba7b:bd17. Groups of numbers that contain all zeros are omitted to save space when viewing the address, leaving a double-colon separator to mark the gap, such as fe80::46fe:3bff:fef6:d115.

Each of your devices at home will connect to the router, and the router will allocate an IPv4 and IPv6 address from its available pool of addresses. The router itself has its own IP address which it connects to the ISP with, of which the ISP will have purchased large groups of IP addresses from the IANA (Internet Assigned Numbers Authority).

Form a Layer of Security to Protect Your Home Network

Your router will contain a built-in firewall, which is designed to help stop unwanted access to the devices on your home network. For example, a hacker from the Internet will need to get past your router's firewall security before that can access your home network.

Offer Wireless Connectivity to Devices

Quite an obvious one this. The router will have built-in protocols and antennae to communicate and allocate IP addresses to any wireless devices that have cleared the password stage.

A Built-in Switch, so Multiple Devices can Connect via Ethernet Cables
Most routers will feature a four-port switch (more on switches later), that allows multiple wired computers and devices connection to the router. The switch will automatically sense the network speed of the device connected and communicate with it accordingly.

Network Address Translation (NAT)

Network Address Translation translates the IP addresses of computers in the home network to a single IP address. That single IP address is part of the ISP's range of addresses. Basically, NAT conserves the number of public addresses used within an organisation, and it allows for stricter control of access to resources on both sides of the router.

For example, a device inside a network makes a request to a computer on the Internet. Routers within the network recognise that the request is not for a resource inside the network, so they send the request to the firewall. The firewall sees the request from the computer with the internal IP. It then makes the same request to the Internet using its own public address, and returns the response from the Internet resource to the computer inside the private network. From the perspective of the resource on the Internet, it is sending information to the address of the firewall. From the perspective of the workstation, it appears that communication is directly with the site on the Internet. When NAT is used in this way, all users inside the home network access the Internet with the same public IP address. That means only one public address is needed for hundreds or even thousands of users.

Resource Sharing

As the router connects all the devices to the same network, they are all able to intercommunicate with each other, and therefore share resources. For example, all devices can print to your home's networked printer.

Parental or Safety Controls

More modern routers now offer better parental controls to help curb the amount of time younger people have access to the Internet. Also, they can be used to limit the websites that younger people can have access to.

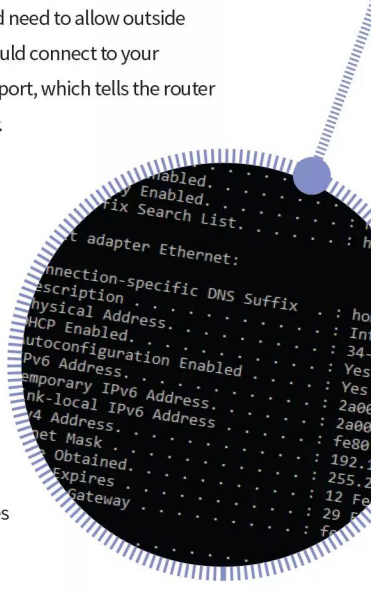
Port Forwarding

Port forwarding is another behind the scenes process that the router takes on. It intercepts traffic to and from home networked devices to the Internet and can redirect them to a specific device on the network.

All network connections include a port number, Port 80 is used for HTTP requests, and these ports define what the service is. For example, if you want to host a Minecraft server, you would need to allow outside Minecraft users access to your server. They would connect to your Router's IP address and the specific Minecraft port, which tells the router what computer is hosting the Minecraft server.

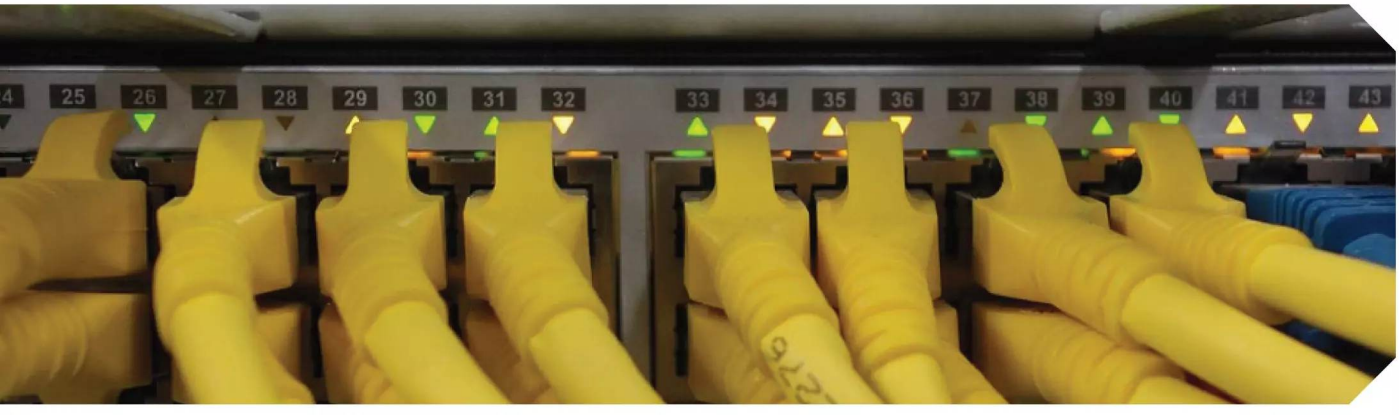
Upgradable Firmware

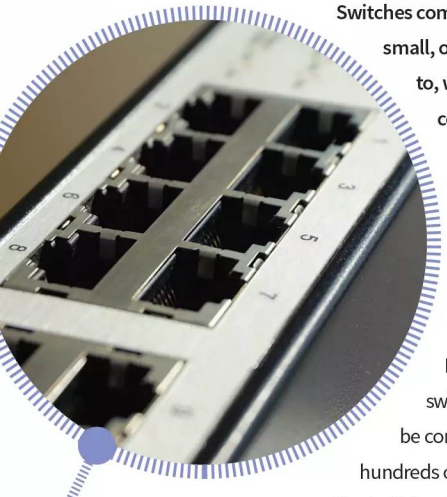
As telecommunications protocols advance, and as security flaws are discovered, an ISP has a responsibility to ensure that all the routers it has sent out to its customers are up-to-date. The ISP can do this by automatically upgrading the software on the router, called the firmware. The new firmware will contain updates, patches and upgrades to security, and will add new features and improvements to the router.



Switches: What are they, how do they work?

Most modern routers contain at least a four-port switch built into the back of the unit. These ports allow for physical, Ethernet connection to the router from networked devices. But what are they, and how do they work?





Switches come in many sizes. Some are quite small, offering just a few ports to connect to, while others, used mainly by companies, can have tens of ports. In the simplest terms, a switch enables multiple computers to connect to a network using a physical cable, called an Ethernet cable (or RJ45 cable).

Each computer is connected to the switch, and multiple switches can be connected to each other. This allows hundreds of computers, let's say on the floor of an office building, to be connected to the floors above and below, as well as to the company's servers and routers.

Switches also come with different backbone speeds, which is the physical limit the data can travel to and from each of the ports. These speeds range from 10Mb/s, to 100Gb/s. The most popular, and the one that's likely built into your router, is 1Gb/s; although 100Mb/s is still possible to find on some routers. While Ethernet is the primary connection port type, a lot of switches will also have fibre port connections too, which is much faster. This allows multiple switches to connect to each other and form a much faster bandwidth backbone connection.

The primary function of a switch is to transport data around the network, usually from areas of the network that are out of reach from its core. For example, you can have all your computers connected to your router's switch, but if you want the computers upstairs connected, you'll need to factor in a switch. You would purchase a switch with the required number of ports, use one of the ports for a cable that will run downstairs to the router's switch, then connect your upstairs computers to the new switch. You've now created a multi-switch network; the one upstairs is connected to the switch that's built into the router, and all the computers can happily gain access to the network and the Internet.

That's a very simplistic example, but it's not too different from how a real-world situation will work. In the office you would have multiple floors, teams, rooms and so on. Each of those probably has its own switch, which is in turn connected to the main switch that the company's servers are connected to. Naturally, depending on the size of the company and how

many computers, printers and so on are connected to the network, the setup can quickly become quite large, involving many switches across multiple floors and even buildings.

Managed Networks

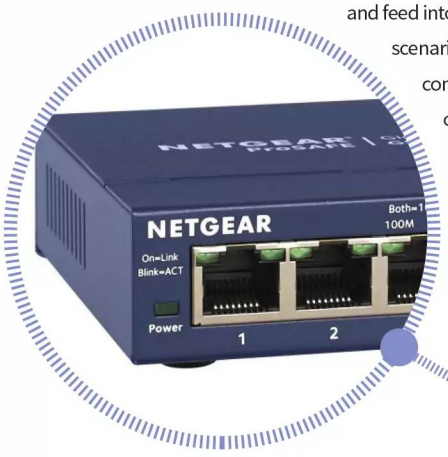
Another core function of a switch is to manage the network. This means that a switch is capable of building a map of its connected devices, and ensuring that the correct data is sent to the correct device in as little time as possible, and as cleanly as possible by the shortest route.

A good example is if computer A needs to send something to Computer B. Both computers are located in different parts of the network. A switch is able to monitor and deliver the data package from computer A directly to computer B without having to interrogate any other connected device on the system. Should computer A or B be moved in the future, the switch can intelligently alter its understanding of the location of the devices and change the route accordingly; building a map of the network for better efficiency and avoiding packet collisions on the network, which will greatly degrade the overall speed of the network.

The types of switches found built into routers are usually unmanaged, but this doesn't mean they don't manage the network to some small degree. An unmanaged switch will still automatically learn and map the network, avoiding collisions by routing data to its intended devices, they just won't feature some of more complex elements of a managed switch.

Switches at Home

If you have no wireless devices in your home, then using switches to connect all the computers on the network is your best bet. A switch could therefore be positioned upstairs, feeding to the built in switch in the router, another could be located in the garage, feeding to the router, and another could be in your shed at the bottom of the garden, again feeding into the router. The router will now be lacking in ports, so one more switch for the downstairs will satisfy any computers connected and feed into the router. In this scenario, everything is connected to each other and ultimately the router. They can all 'see' each other, as well as gain access to the Internet and other network resources.



Layers

Switches also offer different functionality in the form of layers. These layers perform different operations depending upon the layer type, and they generally gain in complexity the higher the layer number.

Layer 1

A layer 1 switch transfers data, but does not manage any of the traffic coming through it, an example is an Ethernet hub. Any packet entering a port is repeated to the output of every other port except for the port of entry. Specifically, each bit or symbol is repeated as it flows in. A repeater hub can therefore only receive and forward at a single speed. Since every packet is repeated on every other port, packet collisions affect the entire network, limiting its overall capacity.

Layer 2

A layer 2 switch is a multiport device that uses hardware addresses, the MAC address, to process and forward data at the data link layer (layer 2). A switch operating as a network bridge may interconnect devices in a home or office. The bridge learns the MAC address of each connected device. Bridges also buffer an incoming packet and adapt the transmission speed to that of the outgoing port.

Layer 3

A layer 3 switch can perform some or all of the functions normally performed by a router. Most network switches, however, are limited to supporting a single type of physical network, typically Ethernet, whereas a router may support different kinds of physical networks on different ports.

Layer 4

Layer 4 switches commonly offer Network Address Translation, improved Quality of Service (QoS) capabilities and may include a firewall, Virtual Private Network connection or higher-level forms of security gateways.

Layer 7

Layer 7 switches can distribute the data load based on the target Uniform Resource Locator (URL), and may include a web cache.

Wi-Fi: What is it, how does it work?

It's not that long ago when wireless communications across the network was akin to witchcraft. At the time we had coaxial cables networking everything, then Ethernet, and then Wi-Fi began to emerge, and it was utterly brilliant.

We take Wi-Fi and wireless connectivity for granted these days. The phone that most of us carry around, with its ability to connect to a network, or Bluetooth pair to another device, is simply an amazing piece of technology. As we said in the intro, it wasn't all that long ago when connecting to a network over a wireless setup was simply out of the question. While it has existed since the early seventies, as UHF wireless packet networking, it wasn't worth the exorbitant cost of installation, setup and maintenance. But Wi-Fi, which stands for Wireless Fidelity, has come a long way in a short time.

In essence, as you already suspect, Wi-Fi is wireless connectivity; the ability to connect to a network and therefore the Internet wirelessly. It's a set of protocols and data packet exchanges that enable a PC, laptop, tablet and so on, to connect directly to a router or other Access Point using a number of available radio frequencies.

These frequencies range from 900MHz, through to the 3.6GHz, 4.9GHz, 5GHz, 5.9GHz, and 60GHz bands; and are called channels. They use a set of protocols called IEEE 802.11, and split into standards such as a, b, g, n, ac and ax. These standards basically denote the age of the wireless device, where 802.11 was the first standard and created in 1997, 802.11a came next in 1999, then 802.11b, 802.11g, 802.11n, 802.11ac and finally 802.11ax. You can also get 802.11p and 802.11ad/ay, but these are reserved for higher rate communications.

Each of these standards connect to a wireless access point, such as your router, at different speeds. 2.4GHz is the most common connection channel and can offer up a theoretical speed of 54Mb/s. Dual-band Wi-Fi devices are able to connect on both 2.4GHz and 5GHz channels, and have a maximum throughput of up to 7Gb/s (although in theory, it's said it can hit 12Gb/s).

With Wi-Fi being constantly updated, there are frequent increases in the connection speed between wireless devices. Generally, an accepted improvement from one wireless standard to the next often means a performance increase of around 30 to 40% from the previous generation standard. There are other factors at work too, such as MU-MIMO (Multi-User, Multiple Input, Multiple Output), which increases the number of antennas in a router for transmitting and receiving data, thus improving the capacity for wireless connections.

Working with Wi-Fi

A Wi-Fi router works by converting the network communications signals into radio waves, then transmitting them around itself, creating its own small Local Area Network; which incidentally is why it's called WLAN, Wireless Local Area Network.

Devices that can pick up and receive the radio signal, such as a tablet or phone, are able to connect to the WLAN and decode the radio waves back into a readable form of network communications. The power of the router's Wi-Fi isn't very strong, and doesn't have a lot of range, but it depends on the frequency being used as to how far you're able to communicate with a router. For example, a 2.4GHz band can reach up to around 150 feet, and 5GHz can reach even further. However, as routers are placed inside our homes there's a lot of interference for the signal to get through. Walls, doors and even some furniture (no, Christmas lights don't affect your Wi-Fi), will rapidly degrade the signal, so while the theoretical distances sound good at several hundred feet, in reality you'll be lucky to get a good signal within thirty to forty feet of your router.

On top of that, the signal will become weaker the longer the distance, and it'll start to drop in power very quickly too. Due to this, your router needs to have several antennae in order to transmit and receive the signal, and they need to be powerful enough to push that signal as far as possible, before it naturally starts to drop.

Interestingly, one of the key features of keeping the signal as clean as possible was created as a by-product of a failed experiment to detect exploding mini black holes the size of an atom particle; and was invented by an Australian radio astronomer called Dr. John O'Sullivan, together with his colleagues Terence Percival, Graham Daniels, Diet Ostry and John Deane.

The Future

In 1929, Nikola Tesla theorised the 'World Wireless System', and he said. "We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do his will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."

Tesla may have had his own personal demons to battle, but you have to admit the man was pretty much on the ball. But what does the future hold for Wi-Fi?

It's been long thought that the future of Wi-Fi will be tighter frequencies, but with extraordinarily boosted power. This extra power will be able to cut through most of the obstacles that face current Wi-Fi frequencies, and through the use of more secure roaming hotspots, we'll be permanently connected to a Wi-Fi network as we move around.

There are even concepts being worked on by communications companies to eventually remove wired telephony, and instead our home routers will communicate directly via Wi-Fi to the ISP.

Of course, all that is some years off. Until then, we'll enjoy the ever increasing speeds of Wi-Fi and its ease of use in our homes.

Powerline Adapters: Extend Your Network

If your home network doesn't reach the furthest corners of your house, maybe because some rooms are too far from the router, or a thick stone wall blocks your Wi-Fi signal, powerline adapters are a potential solution. But what are they, and how do they work?

There are many reasons why your home Wi-Fi network doesn't reach into every part of your house. The router's wireless signal might not have the range to get to the furthest rooms, or the walls might be very thick and heavy, which makes it difficult for Wi-Fi to penetrate. So maybe you need to make a cabled connection to one of the router's Ethernet ports, but don't want to trail Ethernet cables through the house. Powerline adapters are a potential solution for extending both your wireless and cabled network, using your home's electrical cabling as data cables.

A powerline adapter kit comes with at least two plug adapters, which are small devices that plug into your electrical sockets. They usually have at least one Ethernet port, and they might also have Wi-Fi access points and 'through ports', whereby you can plug an electrical device into the adapter, and thus use it without losing a socket. One of these plugs should be fitted near your router. Plugs with through-ports are very useful here, as you can plug the powerline device into the mains, then plug the router into the powerline adapter. An Ethernet cable – which should be supplied with your powerline adapter kit – should be used to connect the adapter to the router. The second powerline adapter should be positioned elsewhere in the house, somewhere your current home network can't reach. A little more setting up might be necessary, probably using free software supplied by the powerline adapter's manufacturer. When you're done, the two powerline adapters communicate with each other and can transfer data between them, using the household electrical cabling as data cables. If the adapter that's not connected to your router offers a Wireless Access Point, a Wi-Fi enabled device can connect to it and get online (and also onto your local network, of course), by connecting wirelessly to the powerline adapter. This adapter then connects to the router's powerline adapter, through the house's electrical cables, and thus to the router. It sounds complicated, but it isn't. It just works.

Cabled Connectivity

While most Internet devices connect to your router using Wi-Fi, for some things, you might prefer a cabled connection. A games console, for example, might benefit from the additional stability offered by Ethernet, and if your TV shows regularly buffer due to congested wireless networks, plugging in an Ethernet cable might solve your problems. If your router is close enough to the device in question, there's no problem; simply connect the two with an Ethernet cable. Unfortunately, this is often not the case. The console or Smart TV might be a long distance from the router, quite possibly in a different room entirely. This is where powerline adapters come in handy.

Instead of trailing Ethernet cables through the house, and drilling holes in the walls to pass them through to the next room, you can use a powerline adapter setup. With an adapter connected to your router, you simply need to plug the second unit near the device you want to connect through

Ethernet. You then connect the console, TV, video streamer or other such device to the nearby powerline adapter with another Ethernet cable. Your house's electrical cables are used as a continuation of Ethernet, and your device enjoys a cabled connection to your router.

Wireless Connectivity

Problems with wireless networking are common, and are usually caused by the router not reaching the furthest corners of your house, creating blindspots. In older houses, heavy brick walls might reduce the router's wireless reach. Whatever the reason, if you need wireless connectivity in a place where your Wi-Fi network is weak, or even absent, you can use powerline adapters to get around the problem.

With a powerline adapter that offers a Wireless Access Point, you can make a Wi-Fi connection to the adapter, which reaches the router through the other powerline adapter and your household electricity cables. Data is sent between the adapter connected to your router and the one positioned in a Wi-Fi blackspot, in any room in the house. If your powerline adapters offer mesh Wi-Fi, it's completely seamless. There's no need to disconnect your wireless device from the router and reconnect to the powerline adapter's Wi-Fi as you move around the house, as it's done automatically.

Adding More Adapters

Having set up your first two powerline adapters, one on the router and the other somewhere else in the house, you can add more if you wish. They all connect to the router, and to each other, through your home electrical cables. Some powerline adapter packs contain more than two adapters to begin with, but if yours doesn't, you can always buy more units and add them to your network if needed.

In the early days of powerline adapters, almost all devices conformed to the HomePlug AV standard. You could therefore mix and match adapters from different manufacturers, as they were all compatible with each other. This is less true today, as all sorts of different standards have sprung up. We recommend, therefore, that you stick to the same brand when adding more plugs to your powerline adapter network.

A Typical Powerline Adapter

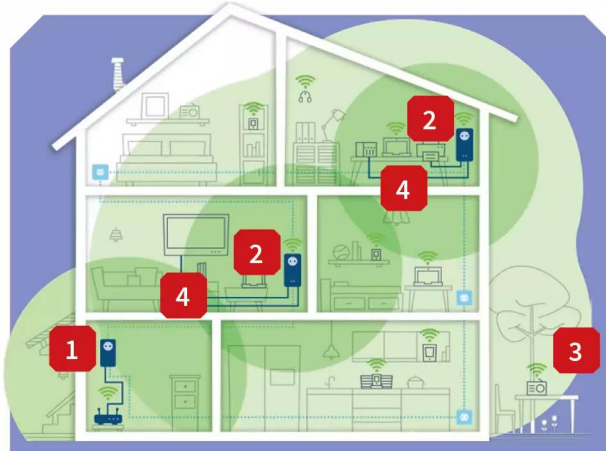
There are many brands of powerline adapter available. This one is by devolo, but other manufacturers' devices are of a similar design.

1 Start by plugging the powerline adapter into a mains socket. This one's a British three-pin plug, but adapters with EU and US plugs are available.

2 This particular model has a through-port, so you can plug in another electrical device. This means you can use the powerline adapter without losing an electrical socket.

3 This particular device has two Ethernet ports. Some models have more, and powerline adapters that are only wireless extenders might have none at all.

4 As you can see from the 'Magic WiFi' brand and the wireless button, this device offers a wireless access point as well as Ethernet connectivity.



How Wi-Fi Mesh Works

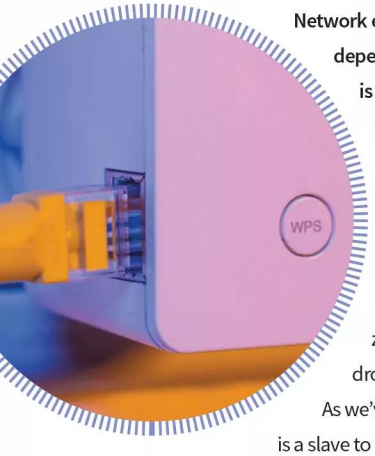
If your router's Wi-Fi network doesn't cover the whole house, powerline adapters that offer Wireless Access Points are a solution. First, plug the base unit into the mains (the dotted blue line), and connect it to the router using an Ethernet cable 1. You can then add Wi-Fi adapters anywhere in the house 2, by also plugging them into the mains. They greatly extend your wireless reach by creating a 'mesh' with the router's own Wi-Fi signal 3.

The same passcode allows you to connect to the network anywhere within this mesh. If you move from room to room, maybe with your phone in your hand or to use your laptop elsewhere in the house, you don't have to disconnect from one access point and log into another.

As most adapters come with Ethernet ports, you can also use them for cabled connections; the solid blue lines 4.

Network Extenders: What are they, how do they work?

If the cabling option, together with powerline adapters, doesn't work for you, then you can easily expand the reach of your Wi-Fi network by utilising wireless extenders. They're cost-effective and easy to setup.

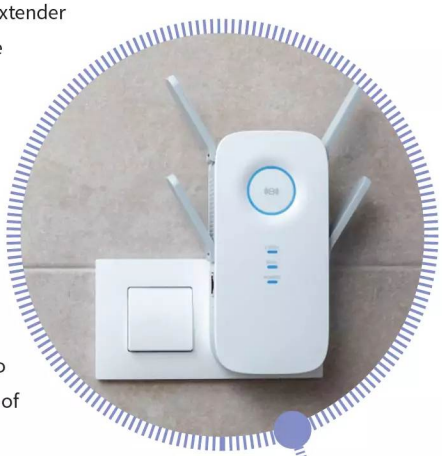


Network extenders fall under different names, depending on who you talk to or what company is selling them. They can be called wireless extenders, signal boosters, Wi-Fi range extenders and so on, but effectively, they all do the same thing: extend the signal of your available Wi-Fi network.

Most houses will have one or more dead zones, where the Wi-Fi signal from the router drops to the point of being virtually useless. As we've mentioned previously, the Wi-Fi signal is a slave to its environment and can be affected by walls, furniture, microwave ovens and all other manner of objects we regularly use throughout the home. If you have your router in the front room of your house, for example, then the upstairs back bedroom may prove to be one such dead zone, due to the Wi-Fi signal having to get through several walls and a floor.

A network extender can solve that issue by acting as a bridge between the devices needing access, and the router's ever-weakening Wi-Fi signal. There are different forms of network extender available, but the vast majority are similar to that of a powerline adapter: a plug-in device.

You need to plug the network extender into a free electrical socket, use its accompanying software to locate it and connect it to your existing Wi-Fi network - and away you go. While it's powered up and the network is up and running, it will extend your Wi-Fi signal by as far again as the router's signal, thus giving you access to even the most obscure corners of your house and property.



Mesh

Mesh is a term that's now being used together with a lot of Wi-Fi routers. Many routers these days come with an included Mesh node – which is to all intents and purposes a Wi-Fi network extender.

Mesh is a network topology that's designed around interconnecting nodes. These nodes can be switches, routers and so on, that are directly connected to as many other nodes as possible and cooperate with each other to pass data across the network in as effective way as possible. They're able to manage workload and bandwidth, and alter the routes for data to take should any of the nodes fail and drop off the network.

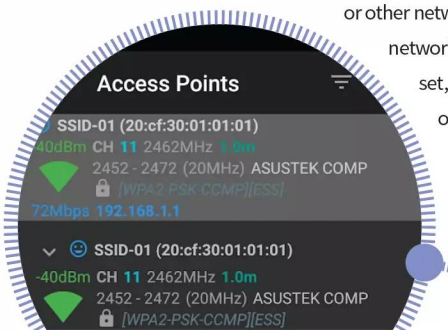
A wireless Mesh network works the same way, but exclusively uses Wi-Fi signals to form the network. A lot of ISPs have now adopted the term Mesh into their products, and will include a Mesh disc, or node, with their router.

These nodes can be placed in dead zones around your home and property and connect directly to the router. The end result is a very large Wi-Fi signal range for a single network, extending throughout the home and well into the garden and surrounding property.

The beauty of this setup is that any laptop or other Wi-Fi device can be moved around the Mesh signal range and quickly jump from one node to the next without any indication of a loss of signal. In fact, the user probably won't even notice that the device is hopping from one node to the next.

Multiple users are also catered for, as the Mesh setup allows for effective load balancing across all the available nodes. If a single node is having to deal with a lot of bandwidth and users, then other nodes can quickly take charge and take the strain off the first node. Of course, this is providing the other nodes are within range of the users.

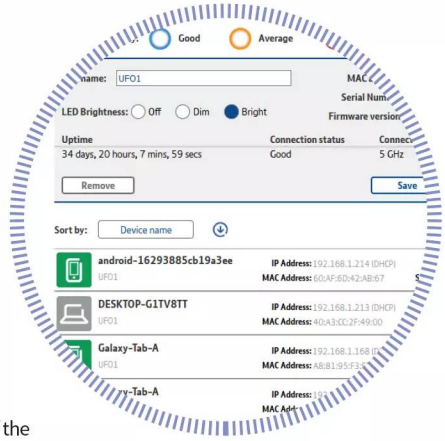
Guest networks are also easy to setup in such a configuration. A user could create a free-to-use mini network that allows access to the Internet or other network services. The guest network can have certain limits set, such as connection times or bandwidth caps; it's all up to the user who is setting it up.



Effective Setup

When setting up a wireless network extender you need to consider its placement for best effect. For example, having your router in a corner of the house isn't a very effective setup, as half the Wi-Fi signal will be broadcast outside. The perfect place for a router is somewhere in the centre of the house, where the signal is spread out through the house and not wasted outside.

Of course we can't always help the location of the router, since they generally need to be placed at the main telephone port. What you need to do in these circumstances is download a Wi-Fi analyser for your phone or tablet.



A Wi-Fi analyser will indicate the signal strength of the connected Wi-Fi network as you move around the house and surrounding property. Where the signal begins to drop, and any dead zones you find, you can mark and place a network extender or Mesh node.

After some thorough analysing of the Wi-Fi network, you will end up with a wireless local network that doesn't have any dead zones and is being effectively boosted at the appropriate locations. You can always review the placement from time to time, and add or take away nodes and extenders as your network and its devices change.

Get Extending

If you've got more wireless devices on your network than wired ones, then investing in a set of network extenders makes good sense. Your network will be better managed in terms of use and bandwidth, and you won't have the inconvenience of having to move to another location in the property for a better signal.

Getting The Most From Your Wi-Fi

Wi-Fi is much like electricity, you don't think much about it until it's not available. There's a lot you can do with a good wireless network, so this chapter will look at how you can get the maximum potential from your Wi-Fi, from creating a wireless network plan, to surveying your home to find Wi-Fi dead zones.

Want to discover how to secure your wireless network, while also extending it to the outer reaches of your home and property?
Then this chapter will help you become more Wi-Fi knowledgeable.

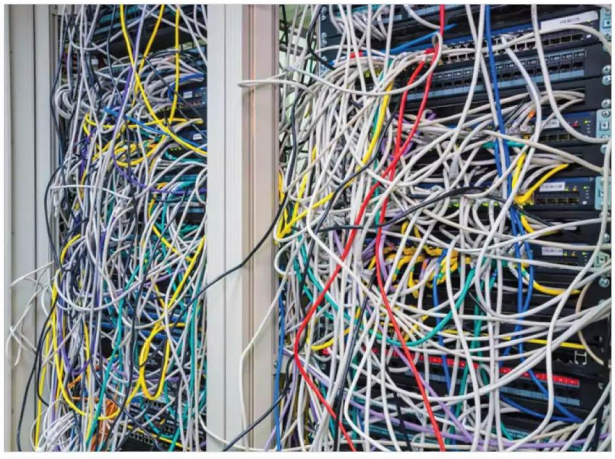
Benefits of a Wireless Network

As most routers these days come with a Wi-Fi setup and perhaps several Mesh nodes out of the box, it's easy to assume that the whole world wants you to go wireless. For those of you who are wary of Wi-Fi, though, here's ten good reasons to consider wireless over wired networks.

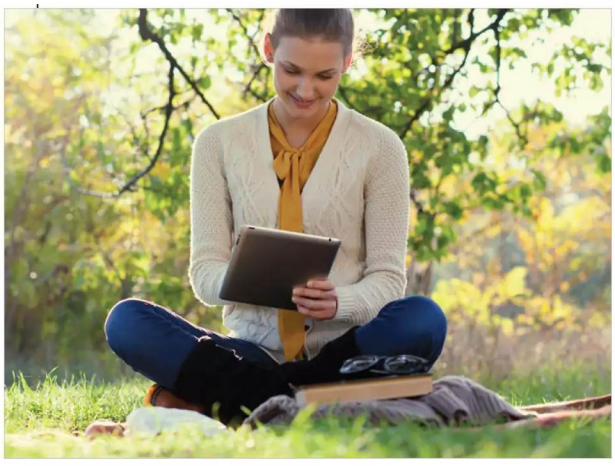
BENEFIT 1 **EASY SETUP –** The beauty of a wireless network is that it's remarkably easy to setup. Once you've got your router and any network extenders you need, it's a simple case of pairing everything up with the router and you're up and running.

BENEFIT 2 **EASILY MAINTAINABLE –** In addition to an easy and quick setup, maintaining a wireless network is a similarly easy process. If you find any dead zones, through using a network analyser, then you can fill the gaps in the signal with another extender. And you can revise your setup without too much effort.

BENEFIT 3 **NO MESS –** One of the main benefits of going wireless throughout is the fact there's no ugly wires dangling, or stuffed behind the equipment. Setups like a home entertainment system can be networked with just the power cables for the devices themselves, and not lengths of Ethernet cables.

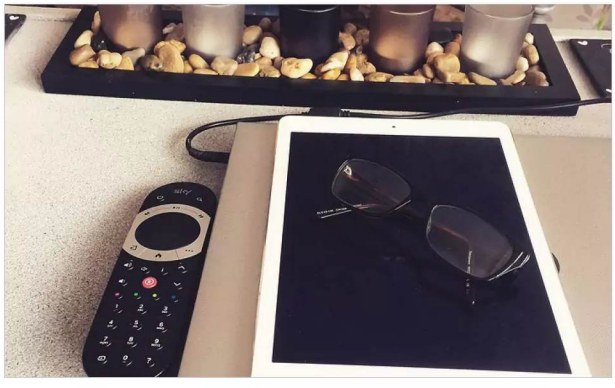


BENEFIT 4 **INCREASED MOBILITY –** Having a good wireless setup means you can work from any location within your signal range. Naturally you can still sit at the computer, but you're free to roam the house; perhaps even do a spot of work while lounging in the sun in the



BENEFIT 5 **INCREASED SCALABILITY –** As an element of the maintenance and setup benefits, increased scalability of your wireless network means you can expand and extend the signal as your needs arise. If you want to include the shed at the bottom of the garden, for example, it's a reasonably easy job to get the Wi-Fi beyond the home.

BENEFIT 6 **DECREASE SCALABILITY –** And on the flip-side of the previous benefit, should you wish to downscale your wireless network – perhaps the kids have finally moved out and there's less devices on the network – then it's a similarly easy job to remove elements of the network and shrink the signal.

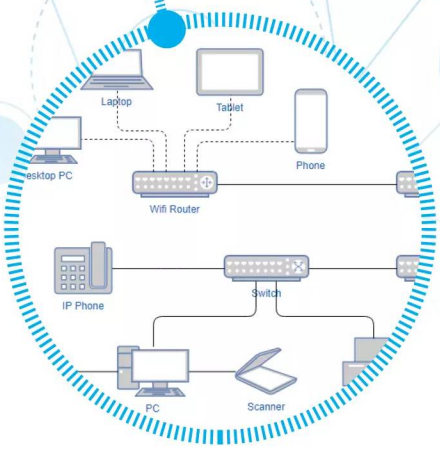


BENEFIT 7 **IMPROVED TECHNOLOGY OVER TIME –** The technologies behind Wi-Fi are ever-improving. Each year brings a new router or extender with more features, better signal strength, more bandwidth and so on. If you go all wireless for your network, then you're going to benefit in the long run from better tech.

BENEFIT 8 **COST SAVINGS –** In general, most wireless networking equipment costs less than wired equipment. Mostly, though, the cost savings are due in part to the need for less networking equipment to get all the devices on the network. Consider the number of switches you may need to connect ten computers. The same can be done with a single Wi-Fi extender.

BENEFIT 9 **EASY REPLACEMENT –** Should you decide to change ISP, or replace your ISP provided router for a more feature-rich model, then all that's necessary is to change the access for each of the extenders and devices on the network.

BENEFIT 10 **SECURITY –** While a Wi-Fi network is prone to more attacks than a wired setup, the security benefit is that you're able to see what devices are connected to your network by name. If you name all your devices logically, then should something you don't recognise appear on the network, you can assume it's someone trying to gain access.



Making a Plan

Before you purchase any number of wireless network extenders and other such technology, it's best that you begin by making a plan of action. Where do you want your Wi-Fi signal to reach? How many extenders will you need?

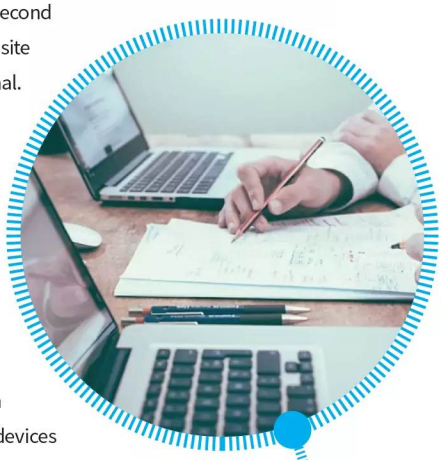
Let's assume you're building your Wi-Fi home network from scratch. You've received the router from your ISP, and you're ready to begin the setup process. It's best not to dive in and set everything up, without first planning what you're going to do. You may reach a point in the setup process where you need to alter something, sending you back to square one.

Making a plan saves a lot of problems later on, and once you have your network setup and ready, and operating to its maximum, you can easily extend it when you need to, without having to pull equipment apart or rearrange devices.

Planning

The first item you should put on your plan is router position. At this point in time you're not able to effectively conduct a wireless site survey with a network analyser, since the router isn't up and running. The router is the core of your wireless network, so it makes sense that it's going to be located somewhere in the middle of your home.

The ideal placement for a wireless router is usually downstairs, as close to the centre of the house as possible, so that the signal is beamed throughout the house and not lost to areas outside. While it's not always possible to position a router in the middle of the house, due to the positioning of the master telephone socket, you can opt for a telephone extension cable, or ask a telephone engineer to relocate the master socket.



Once the router is in place, the second item on the plan is to conduct a site survey of the current router signal. Download a network analyser from your device's app store, and start it up. As you move around the house, make a note of all the locations where the signal is dropping to the point of virtually no connection, or very low. Compare these dead zones with where you're going to be using devices

– for example, a dead zone might be in a closet, so logically speaking you won't be needing to use any devices while in there.

Once you've got a map of where the dead zones are, you can begin to start planning what network extenders are going to be needed. Don't forget to include any outbuildings in your survey, and areas of the garden where you're likely to sit on nice days and possibly work, or just use a Wi-Fi device.

With regards to network extenders in your plan, it's always best to buy extenders that operate at the best possible bandwidth speeds, while still being compatible with your router's Wi-Fi technology. The information that comes with the router and the extenders should provide you with everything you need to know.

Next item on the plan is the installation of the network extenders. As you plug in each extender to cover a dead zone, and extend the network to otherwise unreachable areas, take the time to set them up, and test the coverage with the network analyser. Once all the network extenders are in place and connected, it's time to include one more site survey. This final survey is there to ensure that your network is reaching the places you need it to, such as the garage and other outbuildings.

Next on the plan should be a working test of your newly setup wireless network. Grab a tablet or laptop, and find some bandwidth heavy content – such as a 4K YouTube video. While you're playing the video, move around the house and into the previously surveyed dead zones. Take it outside and ensure that the video is still being streamed while you move around the property and outbuildings.

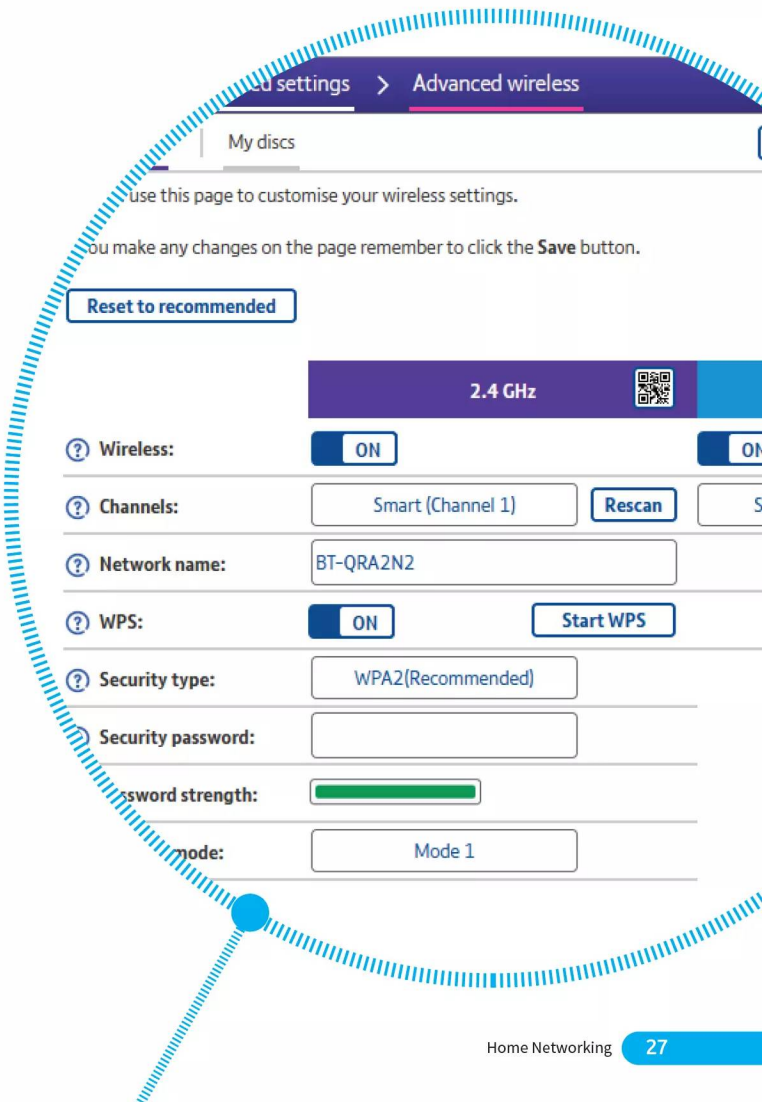
Now that the connectivity is working well, it's time to review the security of your wireless network. Log into the router, and make sure that you're using the latest security method; which is currently WPA2 for most home routers. Also check that the Wireless Mode is set to 1 (providing your router uses Wireless Modes). The Wireless Mode option allows connected devices to utilise the best performance and security features of the router.

Ensure that the security password for accessing the wireless network is strong. It's also recommended to rename all your devices that will connect to the network, so you can easily identify them when you're looking at the connected devices page on the router. If you see a device you don't recognise, then you can quickly isolate it and deny it access until you find out who or what it is.

When you're satisfied that your wireless network is up to scratch, you can finally start to enjoy using it. It's recommended that you take a survey every couple of months to make sure that the signal isn't being degraded over time, due to a faulty device, and that it remains working in tip-top order for you.

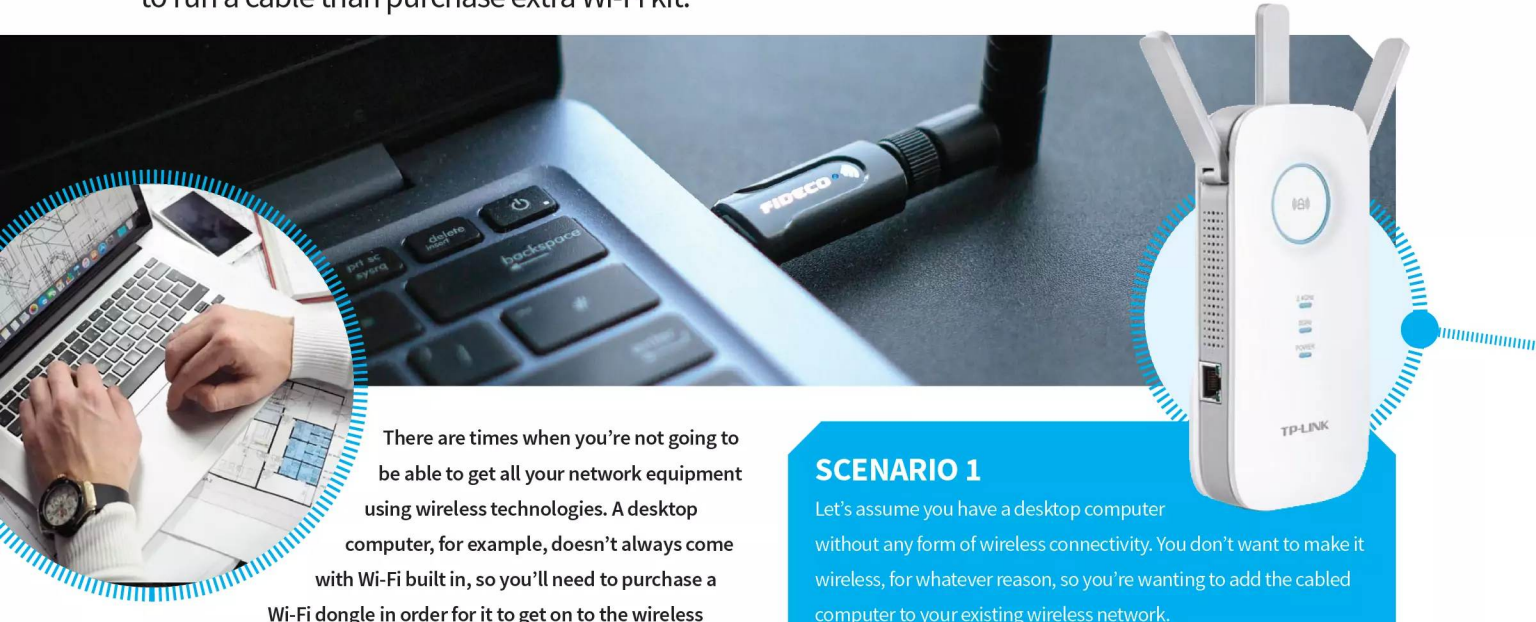
Dynamic Plans

This is, or course, a very simple plan. Your plan may contain other elements that you want to include on your network, such as individual user access, guest access and maybe even separate networks for different devices. The plan is unique to you and your setup, so take your time and make a note of everything you think you'll need to cover.



Wireless to Wired and Back: Creating a Wireless Backbone

While having every component on the network communicate via Wi-Fi, it's not always possible or an effective way to work. Some devices work best when using Ethernet, sometimes it's just easier to run a cable than purchase extra Wi-Fi kit.



There are times when you're not going to be able to get all your network equipment using wireless technologies. A desktop computer, for example, doesn't always come with Wi-Fi built in, so you'll need to purchase a Wi-Fi dongle in order for it to get on to the wireless network. If you use some older equipment, such as an older laser printer, it may only have an Ethernet or USB port available. The same goes for Network Attached Storage (NAS) drives, most of these only come with Ethernet support due to the high bandwidth they tend to use over time. In such cases, you have no choice but to go wired.

Best of both worlds

There's nothing wrong with having wired elements on your wireless network. Essentially, the backbone of the network, the communications to and from the router, will be handled by wireless extenders or Mesh nodes, it's just the odd piece of equipment that will need to have some Ethernet cables run to it. Let's look at some scenarios, and how best to set them up.

SCENARIO 1

Let's assume you have a desktop computer without any form of wireless connectivity. You don't want to make it wireless, for whatever reason, so you're wanting to add the cabled computer to your existing wireless network.

The best bet here is to opt for wireless extenders that include one or two Ethernet ports. A good example of one such extender is the TP-Link AC1750 Wi-Fi Range Extender. This is a three-antennae device that can operate at 450Mb/s on 2.4GHz and 1300Mb/s on 5GHz channels, and it features a single gigabit Ethernet adapter. It costs in the region of £50, depending on where you shop, but will allow any wired device access to the wireless network.

All you need to do is plug in the TP-Link AC1750 extender, configure it to connect to your Wi-Fi network, then plug the computer's Ethernet connection directly into the available port on the extender.

SCENARIO 2

What if you have a few pieces of equipment that can only be cabled up, and very few available electrical plug sockets?

A good choice would be the Linksys RE6700 Dual Band Wi-Fi Range Extender, offering both 2.4GHz and 5GHz channel connection, with a data transfer rate of 867Mb/s. It also features a gigabit Ethernet port, and an electrical pass-through, so you don't lose a plug socket and it costs around £85.

While there's only one Ethernet port available on the extender, thanks to the pass-through, you'll be able to add a multi-plug gang together with a five-port (or four-port), switch – such as the TP-Link TL-SG105 5 port Gigabit Switch (priced at around £15). It's then an easy job to cable up the equipment to the switch, then use one of the ports on the switch to feed to the Wi-Fi extender. In this case, anything that's attached to the switch will be able to access the wireless network via the extender.

Back to the Plan

Going from wireless to wired and back isn't as complex as it sounds, but it can be troublesome from time to time, as there's a lot of bandwidth going through a single point of network contact. That's why you need to plan out your network accordingly, and see what devices are going to need to be wired and which can be wireless. In some cases, if possible, it might be best to connect the wired devices to a router or switch (depending on how many there are), that's connected to the router. As long as the Ethernet connections are gigabit, then you'll have the maximum bandwidth to and from the router, to your device.

SCENARIO 3

Getting a NAS drive onto the wireless network can be done in much the same way as the previous scenarios, but a NAS is slightly different.

NAS drives (or NAS units, if you prefer), are essentially mini-file servers. They hold many terabytes of data that's available to all the users on the network to access; simultaneously if necessary. The kind of files that are accessed can be anything from a few word-processed documents, to a 20GB 4K media file. They're also used as backup locations for the computers on the network, so essentially you could have several devices backing up photos and work to the NAS drive at once.

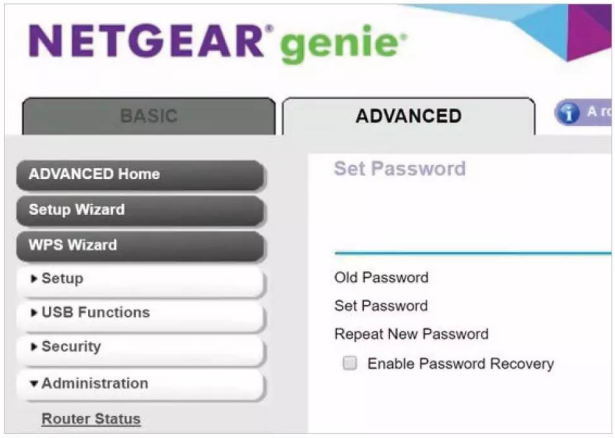
This level of bandwidth usually requires a better connection than normal. In such circumstances as these, it's usually best to directly connect the NAS drive to the router's gigabit Ethernet port. This means there's very little lag between the NAS and the core element of the network. If you were to place the NAS on to a switch, then to a wireless network extender, you're creating two extra hops to the NAS, whereas direct connection to the router minimises the number of networking elements between devices.

Naturally, if it's not possible to get the NAS near the router in order to directly connect it, you'll need to find the fastest possible wireless network extender, with a gigabit Ethernet port, and only connect the NAS to it – nothing else. That way you'll ensure the maximum amount of bandwidth to the NAS.

Improving Wi-Fi Security

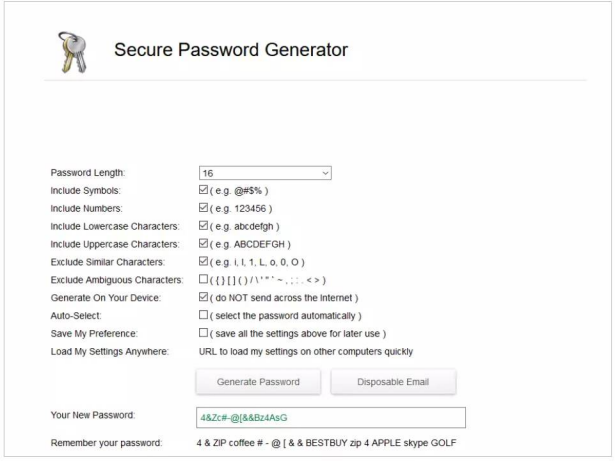
Most routers from an ISP have a reasonable amount of protection enabled by default, however, as with most things of a technical nature, it's possible to improve this further. Here are our top ten tips on how to improve your Wi-Fi security.

TIP 1 **CHANGE ROUTER PASSWORD –** The default password from the ISP to the administrative layer of the router can be quite good, depending on the ISP. Some though are terrible and use the likes of admin/admin as the username and password. If yours isn't up to scratch, create your own strong password using numbers, letters and special characters.

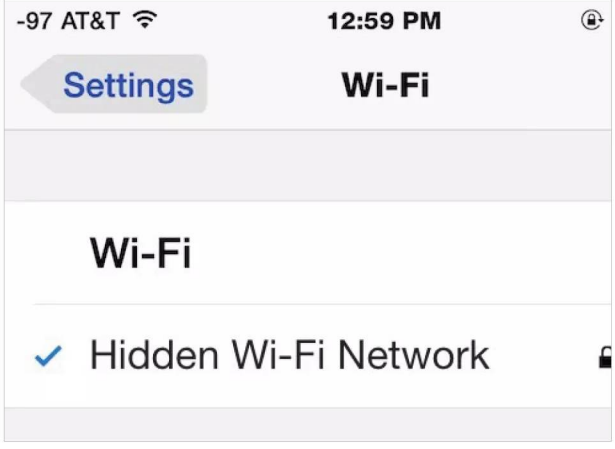


TIP 2 **LIMIT ACCESS –** Although you might find it awkward to do, you should consider saying 'no' when someone asks you for your password. Passing friends of the kids, the neighbour who needs to check something, anyone in who's doing work on the house… the list goes on. Don't give out your password, and it'll remain secure.

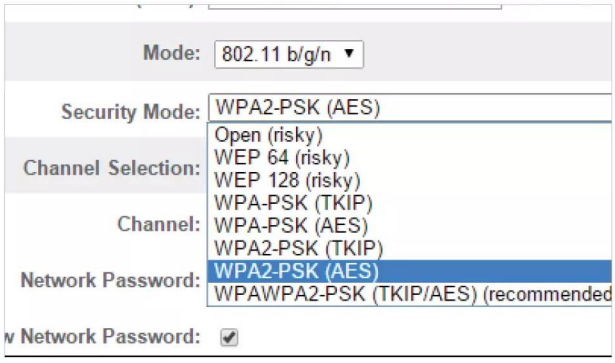
TIP 3 **KEEP CHANGING PASSWORDS –** If you want to remain secure, then routinely change your router's access password. Perhaps keep a list of password reminders to hand, that mean nothing to anyone else, so you can easily pick a strong one to change it to.



TIP 4 **CHANGE SSID –** The Service Set Identifier (SSID) is your router's wireless network name. It's broadcast with the router's signal, so you can find it and connect devices to it. But if you can see it, so can others. Consider opting for the Hide SSID option in your router's configuration (if it's available), otherwise you can use a single underscore with spaces to lessen its presence (_).

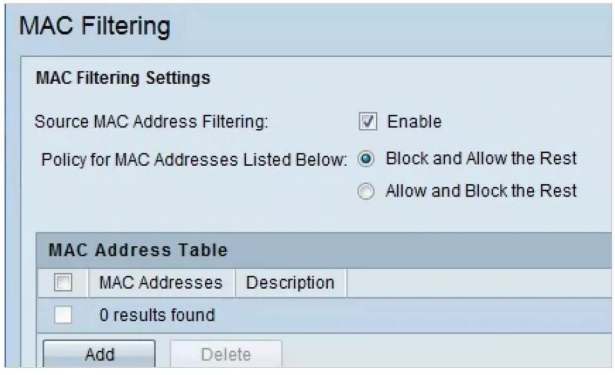


TIP 5 **ENCRYPTION –** WEP, WPA and WPA2 are all encryption types for wireless networks. WEP is the weakest, so ensure that your router is trafficking data on its network with the strongest possible encryption - WPA2. Don't be tempted to go for less to support older hardware.

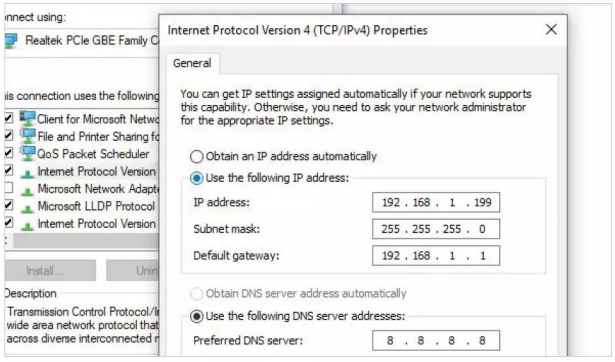


TIP 6 **TURN IT OFF –** If you're not at home, or you're away for a while (maybe on holiday), then turn off your router. If it's not needed, such as remote access to the heating controls or security cameras, turning it off is the best form of security; since no one can hack something that isn't powered on.

TIP 7 **USE MAC ADDRESS FILTERING –** Every network interface has a unique identifier known as a MAC (Media Access Code) address, regardless of whether it's a computer, tablet or games console. If your router supports MAC filtering, you can obtain the MAC addresses for each device and enter them into the router. Only those devices will be able to connect.



TIP 8 **STATIC IP ADDRESSES –** By default your router will allocate IP addresses to any connecting device out of an available pool. If you remove this feature, and use your own addresses, then anyone trying to gain access won't have an IP address to see the rest of your network.



TIP 9 **ROUTER POSITION –** Router position isn't just for the best possible signal. Limiting the router to the middle of the house will benefit not just your wireless network broadcast, but it will also limit access to the signal from beyond the walls of your home.

TIP 10 **MONITOR YOUR FIREWALL –** It's a good idea to keep tabs on what's being added to your router's and computer's firewalls. It's not easy, but not impossible for malicious content to secretly add a route through a firewall for hackers to gain entry to a network.

Getting The Most From Wired Networks

While Wi-Fi is great, it's not as dependable or as stable as a good wired network setup. A wired network is on the whole faster, more durable and not subject to range or obstacles. However, it does come with a few caveats.

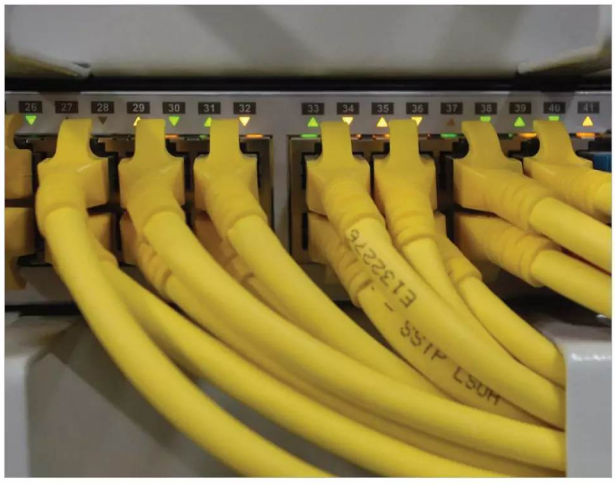
Wires can be messy, so you'll need to plan out your wired setup, and you might need to learn how to make your own Ethernet cables, using specialised tools. However, with this chapter you'll learn how to deal with all these elements, and more.

From planning, to cabling, we'll help you get the most from your wired network setup.

Benefits of a Wired Network

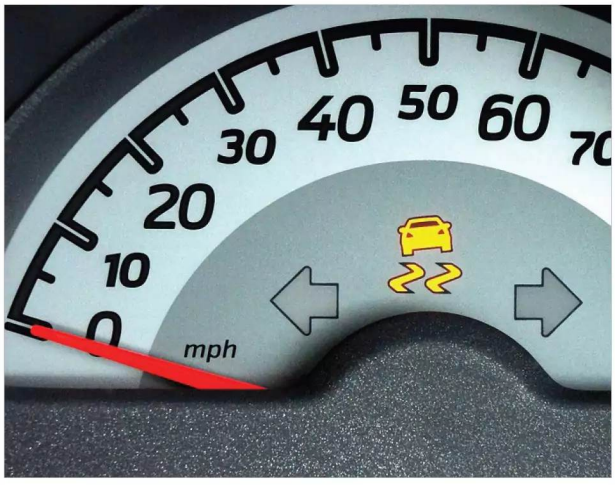
Wireless is a much simpler and neater process to opt for when setting up your network, however, wired networks offer just as many benefits. Here are ten good reasons as to why wired may be better than wireless.

BENEFIT 1 **RELIABILITY AND STABILITY –** When configured and setup properly, a wired network is incredibly dependable. Although wireless technologies are always improving, you'll probably find a wired network more stable and reliable over time.

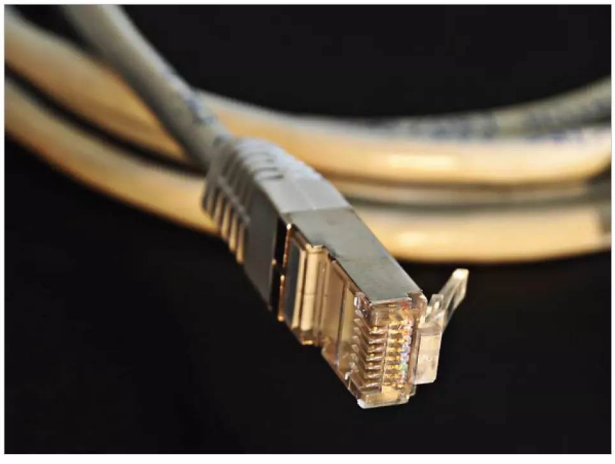


BENEFIT 2 **NO INTERFERENCE –** Wireless networks always have to contend with other elements in its environment, such as walls, other wireless networks, mirrors and even water in a fish tank. A wired network doesn't have those issues. True, you wouldn't run the cable through a body of water – but it's possible with the right cabling.

BENEFIT 3 **SPEED –** Overall, wired networks are faster than wireless. Wireless components on a network may be advertised at speeds faster than 1Gb/s, but other factors have a negative affect on those speeds. Wired Ethernet can operate at 1Gb/s from one computer to the next.



BENEFIT 4 **SECURITY –** A wireless network could potentially have someone nearby quietly hacking into your network. With a wired network, they would need to be physically plugged in to the network in order to gain access to its resources.

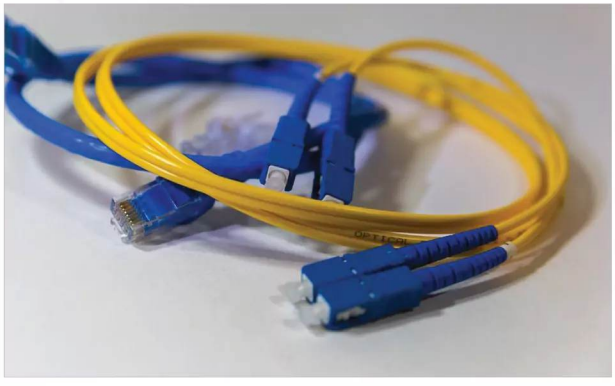


BENEFIT 5 **SECURITY –** A wireless network could potentially have someone nearby quietly hacking into your network. With a wired network, they would need to be physically plugged in to the network in order to gain access to its resources.

BENEFIT 6 **PoE -** Power over Ethernet is a benefit that's often overlooked with wired networks. PoE is the ability for the switch to carry an electrical supply to a device on the network, such as an access point, security camera and so on.

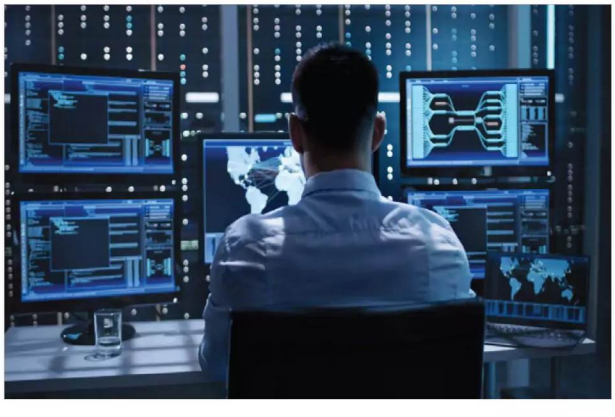
BENEFIT 7 **UPGRADEABLE –** With a wired network, any switches, powerline adapters or the router can easily be upgraded without the need to visit every component on the network to reconfigure it. This saves a lot of time on the part of the user.

BENEFIT 8 **INCREDIBLE BACKBONE SPEEDS –** If you wanted, you could install a wired network that has a backbone speed of up to 10Gb/s, using fibre channels. This speed is incredible, but the downside is that it can cost you an arm and a leg. However, second-hand fibre switches are always being sold somewhere.



BENEFIT 9 **LONGER DISTANCES –** Wired networks can be setup over longer distances than wireless networks. A single Ethernet cable has, roughly, a working limit of 100 metres. So you can have two switches, 100m apart, and the network is sound. To do the same for wireless would take countless extenders and nodes.

BENEFIT 10 **BETTER CONTROL –** With a wireless network you could quickly find there are countless devices having access to your network. With wired, though, you have better control as to what has access, and when it can access the network.



Tools and Equipment Needed

If you're considering going down the wired networking route, then you'll need a number of tools and equipment. Some of these are essential if you're making your own cables, others not so much, but still handy to have around should you need them.

TOOL 1 **CABLE –** You're best off purchasing Cat6 (Category 6), Ethernet cable instead of Cat5 or Cat7. Cat5 is fine, but Cat6 offers better shielding against electromagnetic disturbances. Cat7 is unnecessary at the home networking level. Around 100 metres of Cat6 can be purchased for around £35, depending on where you shop.

TOOL 2 **CAT6/RJ45 CABLE ENDS –** Cable ends are certainly necessary, since you can't plug anything into the Ethernet ports without an Ethernet end on the cable. The prices do vary from place to place, so have a shop around, but expect to pay somewhere in the region of £5 for a bag of ten RJ45/Ethernet cable ends.

TOOL 3 **RJ45 CRIMP TOOL –** In order to clasp the cable end to the cable, to make a good connection, you'll need an RJ45 Crimp Tool. Again, prices do vary, and don't always go for the cheapest model as they can break quickly. However, they're not expensive and can be picked up for around £8.

TOOL 4 **CABLE TESTER –** Although not strictly necessary, a cable tester can save you a lot of bother in the long run. A decent RJ45 cable tester will set you back around £15, but there are far more expensive models available.

TOOL 5 **SWITCH –** The switch you pick will depend on the number of ports you're planning on using. Most will suffice with four or five ports, but eight ports or more might be necessary. However many ports you decide on, ensure it's a gigabit Ethernet switch you're buying. For example, an 8-port Netgear gigabit switch can be had for around £35.

TOOL 6 **POWERLINE ADAPTERS –** Extending a wired network to other areas of the home can be achieved easily with a powerline adapter. Make sure it's as fast as possible, with at minimum a 1Gb/s Ethernet port. A power pass-through is a great feature to have, and will save you a plug socket. Expect to pay around £25 for gigabit powerline adapters, with a pass-through.

TOOL 7 **WI-FI/ETHERNET EXTENDER –** Sometimes it's not possible to run cable, or the powerline adapters may be on a different electrical circuit. In these cases, it's best to extend your wired network via Wi-Fi. You can pick up a Wi-Fi extender with an Ethernet port for around £50-£60; but ensure the Wi-Fi is dual-band, and as fast as possible, and the Ethernet port is gigabit.

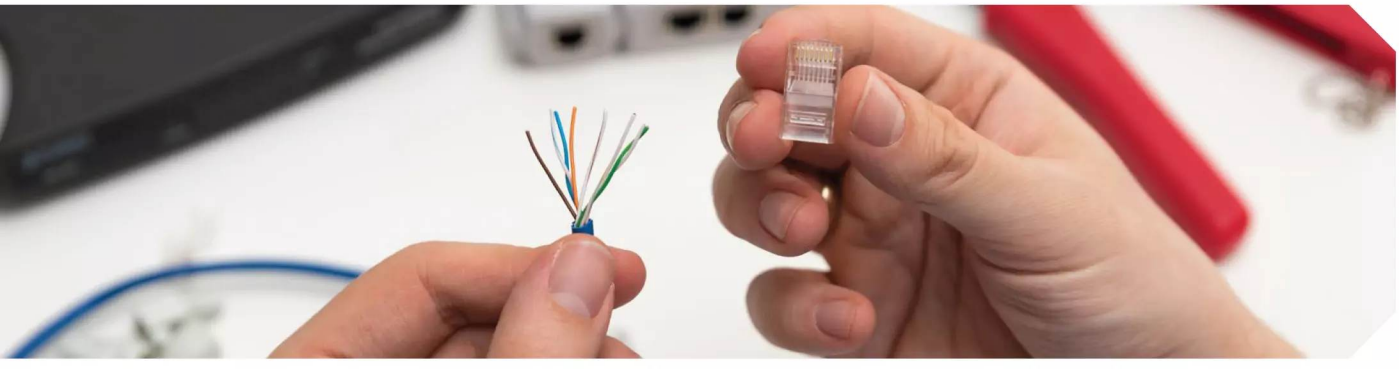
TOOL 8 **TRUNKING –** To neaten up the cabling in your home, consider opting for wall-mounted trunking to hide the cable and create network and power faceplates. Prices vary wildly, from £5 per metre, to £15 per metre, depending on the quality of the trunking. Self-adhesive is the easiest option, though.

TOOL 9 **FACEPLATES –** Faceplates are like plug sockets for networking. They contain one, two or four network sockets that you'll plug your device's Ethernet cables into. Behind the scenes, the Ethernet cable runs through trunking from one faceplate to the next, creating a house-wide network. Expect to pay around £4 for a double-socket faceplate.

TOOL 10 **POWER OVER ETHERNET –** If you're wanting to run the network to something like a security camera, or weather sensor, then you'll need Power over Ethernet. PoE switches offer gigabit connectivity as well as a small amount of power supply for the equipment in question. Expect to pay in the region of £50.

How to Wire an Ethernet Cable

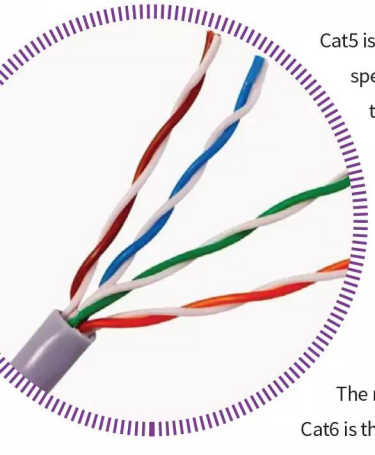
Although you can buy Ethernet cables of differing lengths, there may come a time when you need one that's a specific size. Similarly, if you ever come across a cable with a broken end, you'll need to fix it. Here's how to wire up an Ethernet cable.



Thankfully, you don't need to be a qualified electrician to be able to wire up an Ethernet cable, but you will need some tools at hand before you start. Before we get into the nitty-gritty of wiring, we need to take a look at the types of Ethernet cable available.

Cats

There are two types of Ethernet cable that you'll come across when you're cabling: Cat5 and Cat6. These are Category standard cables types, specifically standard 5 and standard 6. They are both used for networking and feature the same wiring inside the cable.

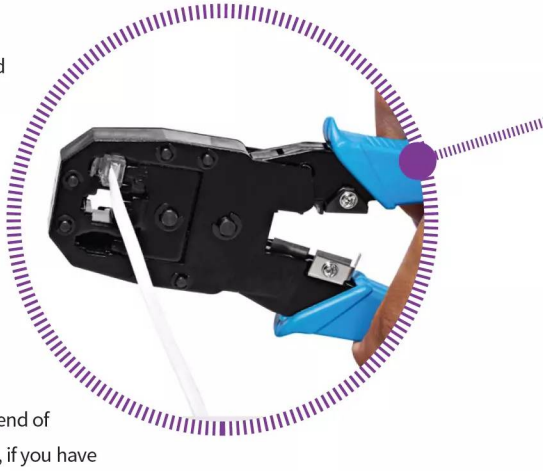


Cat5 is an older standard, but can still transfer speeds to and from switches and routers up to 1Gb/s – although it does have a bit of an issue with holding those speeds over time. Cat6, however, is the newer of the two, and fully supports 1Gb/s speeds over the network, and has the potential for up to 10Gb/s, although that would be pushing the cable's abilities to the maximum.

The main difference between Cat5 and Cat6 is the reduced Crosstalk. Electromagnetic signals that come from Ethernet cables can cause what's known as Crosstalk, when multiple cables are close to one another within a network. The interference caused by cables being too close to each other can slow speeds and also degrade the overall quality of the connection. Increased errors can result from Crosstalk, as well as lost packets. Through the incorporation of a new twisted cable design, and by improving the shielding of the cable, the likelihood of Crosstalk between Cat6 cables is greatly reduced, and therefore a better option.

Cabling

To begin with you'll need to make sure you have enough Ethernet cable, a set of RJ45 cable ends (or plugs, connectors), plastic cable boots, an RJ45 Crimping Tool and, if possible, a cable tester.



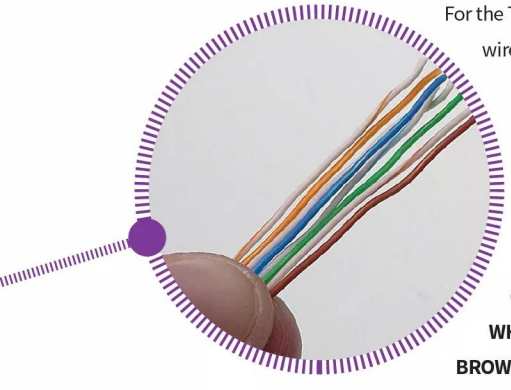
Begin by laying out one end of your Ethernet cable and, if you have one, place the rubber boot over the cable.

The rubber boot isn't important, it will protect the cable end clip from being snagged and broken. Strip off about two inches of the Ethernet cable's plastic sheath. Inside the Ethernet cable you'll see four pairs of wires, twisted into pairs – which is why Ethernet cable is also called Twisted-Pair.

Also, under the cable sheath, you'll notice a thin piece of plastic called the Rip Cord (or Dental Floss, depending on where you are). If you pull this, it will cut through a section of the sheath, allowing you to fold it over and around itself. This will help you cleanly cut away the plastic sheath without damaging the wires underneath. You won't need to use the Rip Cord to slice away much, around half an inch. When you've folded back the plastic sheath, cut it off (called Fluting), and cut the Rip Cord.

The four pairs of wires are broken up into colours: A blue pair, orange pair, green pair and brown pair. Individually they're called white blue/blue, white orange/orange, white green/green and white brown/brown.

There are two standards of Ethernet wiring: T568A and T568B. Most companies and engineers will use the T568B standard (as we understand the US Government requires type A when used for wiring done under federal contracts, however). In short, as long as both ends match, and any wall sockets you plug them into match, then it really doesn't matter.



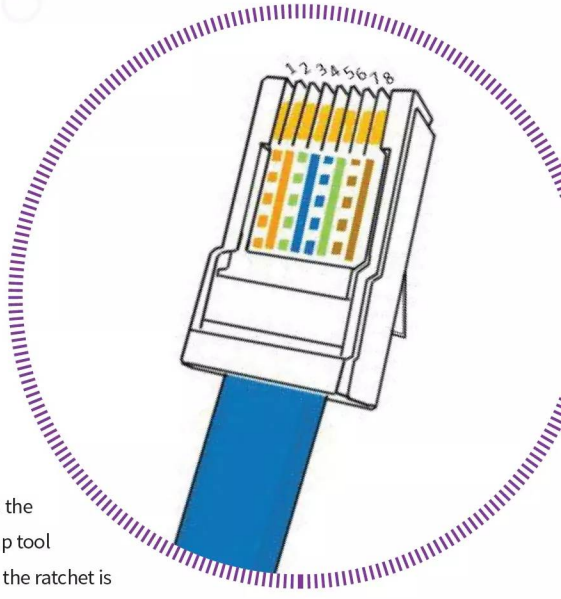
For the T568B standard, untwist the wires into the following order:

WHITE/ORANGE
ORANGE
WHITE/GREEN
BLUE
WHITE/BLUE
GREEN
WHITE/BROWN
BROWN

Now you will need to grab one of the RJ45 cable ends and identify Pin 1. To do so, hold the cable end with the clip facing away from you. Pin 1 is the first pin on the left.

Snip the cable until there's about 1.5-inches free from the edge of the plastic Ethernet sheath. Hold the wires, and arrange them in the order shown above. Firmly insert the wires into the cable end until the copper wire at the centre of each wire is touching the back of the cable end, and ensuring that the following colours match the pins:

PIN 1: White/orange
PIN 2: Orange
PIN 3: White/green
PIN 4: Blue
PIN 5: White/blue
PIN 6: Green
PIN 7: White/brown
PIN 8: Brown



Once the wires are in place, grab the crimp tool, and place the cable end in the appropriate slot in the tool. Squeeze the crimp tool all the way down until the ratchet is released (if it has a ratchet function).

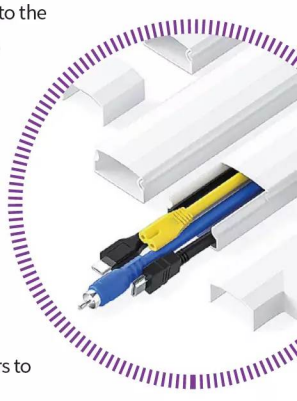
Run the rest of the Ethernet cable out to the desired length, giving yourself a few extra inches in case you mess up one of the ends, and repeat the process to crimp another end on to the cable.

Grab the cable tester, and check your ends. If all's gone to plan you should have a length of Ethernet cable that's good for networking with.

The Extra Mile

You can of course go the extra mile with your cabling, to make it look neat and tidy. But you will need to plan this out carefully.

With your wired network plan, ensure that you've measured the distances to and from the equipment on the network to the router. You can then opt for trunking that will fit to the walls and ensure the cables are neatly hidden, along with having network and power points mounted on the walls, for ease of use.

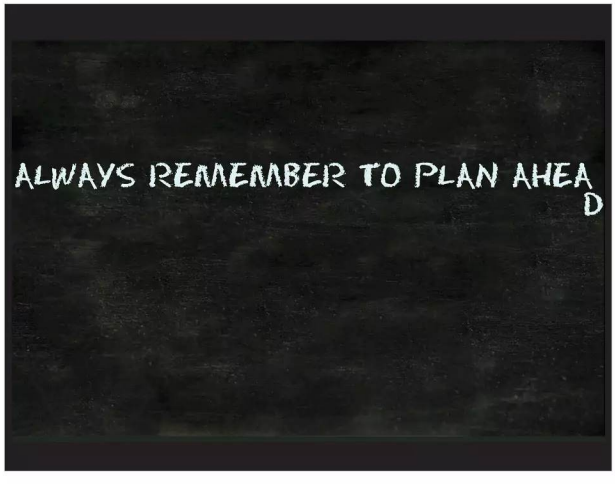


Remember, you might also need to ensure that you can drill through the floor/ceiling to run the cables to the upper or lower floors of your home. In some cases, it's best to opt for good cabling on each floor, with a very good powerline adapter between the floors to extend the network.

Installing Your Wired Network

With everything now ready, tools in place and equipment ready to go, it's time to install your network and get it up and running. Take the time to plan a few preliminary steps, and have everything at hand to ensure it's as easy a setup process as possible.

STEP 1 **PLAN AHEAD –** Take a moment to get a plan together. Where are you going to start, what is the route you're going to take, check the house for potential obstacles you're likely to come across when you're cabling. Have you got powerline adapters and extenders ready?



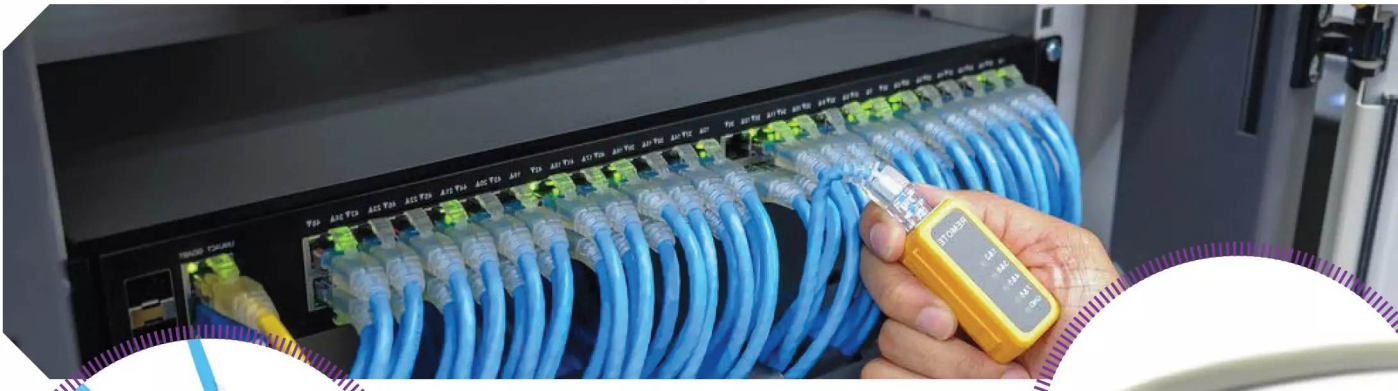
STEP 2 **CABLE ENDS –** If you're plan is looking good, and you've got a route ready, then lay out your cable and start making up the ends. If you're using trunking, make sure it's all cut to size and ready to stick/drill on to the wall.

STEP 3 **SWITCHES –** With the cables all planned out, and the ends being made, make sure that the switches are in the right place, and that there's enough ports to feed the number of devices that are going to connect to them.

STEP 4 **POWERLINE AND EXTENSION –** Finally, make sure that the powerline adapters are in place, plugged in and talking to each other. Plus, ensure that any Wi-Fi to Ethernet extenders are in place, and again, talking to the router's Wi-Fi signal.

The Installation

If you've got a good plan, then the rest of the process should go relatively easily. Be prepared, though, for the inevitable hiccup here and there. The golden rule to networking is: keep it as simple as possible.



If you've taken the time to cable up your own ends, it's always worth just double-checking that they're in good working order. Test the signal with a cable tester, and give the ends a little tug to make sure they're crimped on the cable tightly enough, and won't fall off should you catch them with your feet when under the desk.

When cabling, it's always best to secure it in small lengths. If you've measured the distance to and from one network location to another, such as from the router to a living room switch, then take the time to lay the cable and pin it to the edge of the room (or within trunking), every couple of feet. It might seem like overkill, but it'll keep the cable as neat as possible.

When you run each cable to its switch, or device, it's best to test that device or check the port on the switch to make sure that the connection is working. There's nothing worse than spending all day running several metres of cable only to find you've snagged it somewhere along the line and it's now no longer working. Which means you'll need to trace the cable back and see where it went wrong. If you got loads of cable, then it's even more difficult.

Powerline adapters and Wi-Fi extenders can be the worse offenders when setting up a network. Often they're working perfectly fine one minute, then stop talking to each other when you've completed everything. This happens usually because you've moved something in the way of the signal, in the case of Wi-Fi, so you may need to do a quick Wi-Fi survey again to test the signal strength. As for powerline adapters, they don't often stop working, but they can un-pair with each other when there's another couple of adapters on the electrical wiring. It's a simple case of powering off all the powerline adapters, then powering pairs back up again. They will eventually all 'see' each other and the network will be back up and running.

If you've run cable outside to any outbuilding, make sure that you've marked the location of where the cable goes into the ground, where it's laying and where it comes out. If it's not under the ground, then make sure it's marked where it lies. You don't want to lose connection in the summer due to digging up the garden.

Finally, have fun. Wiring up the house for a home network is a great project. Yes, it can be a bit of a headache at times, and it doesn't always go quite to plan, but it's going to be a solid, and dependable setup when you're done and everything is working.

Networking Home Entertainment

Most of our home network setup is geared towards creating an amazing entertainment system. From 4K smart TVs, with Netflix and other streaming services, to the latest games consoles; and let's not forget the new addition to our homes: AI assistants, such as Google Home.

The home network can be under a lot of strain, so you'll discover how to get the most from them in these coming pages. From the best advice on setting up your home network for entertainment, and what equipment to use, through to setting up and using Google Home, and even Google Stadia.

Networking an Entertainment System

One of the most common setups when it comes to networking is the all-important home entertainment system. This can be as simple as a smart TV and the latest console, or as complex as an entire home theatre setup with AI integration.

Someone's home entertainment system is a very personal setup. While most will have a smart TV, some form of Blu-Ray or DVD setup, and perhaps a games console, others will opt for more exotic components such as Wi-Fi speakers, Google Home automation integration (or some other AI assistant), multiple consoles, a retro games setup via emulation on a Raspberry Pi and much more.

It's impossible to target just one specific setup, but we can make some educated guesses and suggest the best possible way forward for those wanting to get all their entertainment equipment online and talking to each other.

Main Setup

Before we go into depth regarding the individual components, it's worth looking at the base installation first. By this we mean the main networking component that will feed all your entertainment equipment. For most people, the obvious choice is placing the router in the same room as the home entertainment kit – such as the living room. Nine out of ten homes will have a living room that takes up most of the downstairs floor, so having the router near the entrance to the living room will place it as near to the centre of the house as possible. Of course, if you're the tenth house, then your setup will need to be altered.

With a router in the living room, you're in easy reach of its built-in switch ports, as well as having access to a good Wi-Fi signal. You're also cutting down on the amount of networking equipment between the TV, for example, and the router itself.

If you can't have the router in the living room, then in our opinion using a combination of a powerline adapter and a switch is the best option. In this scenario you're able to cable up all the necessary equipment to the switch, which can then feed into the powerline adapter, and in turn can feed into the router via its paired partner. There are other components that may require more networking kit, so let's break some of them down.

TV

All TVs sold now are smart enabled, which means they have the capacity for going online and streaming content. This of course means they'll come with either an Ethernet port or Wi-Fi, or even both. The TV is where a lot of bandwidth is going to be heading, so it makes sense to connect the TV to a gigabit switch – despite the fact that most, if not all, TVs only have 100Mb/s Ethernet ports built into them (despite the manufacturers claiming you need Cat7 cables for the best connection!).

100Mb/s though is perfectly fine for transferring the data needed for 4K and even 8K content, as the TV itself isn't doing anything else other than sorting the data into a viewable image and sound – and its processing can handle the hard work there. For the TV then, an Ethernet cable into

a switch, fed into a powerline adapter is the perfect setup. If not, try and get it working on the 5GHz channel and have it as close to a good wireless network extender as possible.

Games Consoles

The three main games consoles: Playstation, Xbox and Switch are all capable of using Wi-Fi, but only the Playstation and Xbox have an Ethernet port. Surprisingly, all the consoles don't require a fast connection to the home network. Even though there's a lot of data to shift when gaming online, the requirement can easily be met by connecting all the consoles to the wireless network. However, if you want to squeeze the last drops of performance from your connection, then we'd recommend connecting the Playstation and Xbox to the wired network. This leaves the Switch using wireless, which will cut down traffic.

Media Computers/ Retro Emulators

There's a growing number of people who have opted for a media computer as part of their living room entertainment kit. These are often smaller, subtle base units, like the Raspberry Pi, that fit in nicely with the rest of the under-TV equipment, but can still run Windows, Linux or even macOS. These media centres can be used for streaming content from a local device, such as a NAS unit, or via the Internet. They're good for watching YouTube content, gaming and any other duties you'd expect from a computer.

The Raspberry Pi is also great as a retro emulation console, enabling you to play arcade, console and home computer titles from the last forty-plus years. With regards to these, we'd say put them on the wired network, since they're going to use a lot of bandwidth for the content, as well as updates to the OS. As for the Raspberry Pi, again, we'd say wired network, as we've always found the Pi's Wi-Fi lacking when it comes to streaming content. Other new releases such as the Sega Mega Drive Mini are mainly Wi-Fi enabled, and will work seamlessly on a wireless network.

AI Assistants

Most TVs and other entertainment equipment can be controlled with one of the AI assistants, such as Google Home. The AI assistants are all Wi-Fi enabled, and this is perfectly fine. What you're best doing is ensuring that there's a good 5GHz Wi-Fi network extender near to where the AI assistant is located. This will cut down on the traffic on the other channel and improve the bandwidth of the unit.

Blu-Ray/DVD units

While a lot of people use their games console as a Blu-Ray/DVD drive, there are some who either don't have a console or prefer the advanced features a specialised unit can offer. With these units, the connection to the network isn't as important as the connection to the TV, so while they may have Ethernet connections, Wi-Fi will suffice (unless they don't have Wi-Fi access, of course).

NAS

One final element to the home entertainment setup is the addition of a NAS unit. These mini-servers are ideal for storing movies and TV shows, game files that a retro emulator can access and storing a lifetime of digital photos. In an ideal world, you'd have the NAS connected directly to the router's switch, so all traffic to it has the maximum bandwidth. However, if it's not located near to the router, make sure it's connected to a gigabit switch.

Powerline Adapters/Network Extenders

If you're stuck for which one to use for your entertainment equipment, we'd say opt for the powerline adapter (as fast as you can get), and a gigabit switch. The equipment that requires Wi-Fi is probably within reach of the router's signal, and if not, you can add a Wi-Fi extender elsewhere in the room and it'll feed the wireless kit under the TV.

Anything Else (such as a Roku etc.)

Assess the needs of its bandwidth, if it's going to be using a lot of traffic online or on the network, try and connect it to the wired network, otherwise go for Wi-Fi and the best channel/speeds you can.

The Google Home Collection

There are now six different Google Home devices to choose from, including the tiny Home Mini and the new Google Home Hub. The specification and size varies greatly, so if you are not yet sure which Home speaker is best for you, check out all of the details here.

Google Home Max

Key Features: Meet Google Home Max, he helps you to hear every note as the artist intended and feel every beat with heart pounding bass. It's the ultimate speaker, made for your music. The advanced hardware delivers deep bass and crisp treble in stunning stereo sound. It analyses, tunes and updates itself automatically, so all you need to do is listen. The far-field voice control allows Max to hear you across the room, even while the music's playing.
Final Thoughts: The best audio-only based product in the Google Home range.

Dimensions
- Width: 13.2" (336.6 mm)
- Height: 7.4" (190.0 mm)
- Depth: 154.4 mm
- Power cable: 2 m

Weight
- 11.7 lbs (5,300 g)

Colours
- Chalk, Charcoal

Materials
- Acoustically transparent fabric
- Rigid polycarbonate housing
- Silicone base

Supported audio formats
- HE-AAC, LC-AAC, MP3, Vorbis, WAV (LPCM), Opus, FLAC with support for high-resolution streams (24-bit/96 KHz)

Wireless
- Wi-Fi • Bluetooth
- 802.11b/g/n/ac (2.4GHz/5Ghz) Wi-Fi for high-performance streaming
- Chromecast built-in
- Bluetooth® 4.2

Speaker
- Two 114 mm high-excursion (+/- 11 mm), dual voice-coil woofers
- Two 0.7" (18 mm) custom tweeters
- Sealed rigid housing
- Acoustically transparent fabric

Mics
- Far-field voice recognition supports hands-free use
- 6 mic array

Processor
- Quad-core ARM
- 1.5 GHz 64 bit quad-core ARM® Cortex™ A53

Sensors
- Capacitive touch sensor
- Ambient light sensor
- Accelerometer

Power
- AC Power 100-240 V, 50/60 Hz

Ports & Connectors
- USB-C™ • 3.5 mm jack
- USB-C1
- 3.5-mm jack with analogue audio input

AC power
- 1USB Type-C and USB-C are trademarks of USB Implementers Forum.

Operating system
- Android • iOS

Other
- Multi-room audio

Google Home Mini

Key Features: A powerful little helper; Google Home Mini keeps you informed and up to date with instant news, weather and commute updates without lifting a finger. Master the kitchen; Google Home Mini helps with timers, step-by-step recipes, and conversions and substitutes. Start your smart home; it's always improving with seamless connections to the latest compatible smart lights and thermostats.
Final Thoughts: The budget range of Google Home offers a great product for the price.

Dimensions
- Diameter: 98 mm
- Height: 42 mm (1.65")
- Power cable: 1.5 m

Weight
- Device: 173 g
- Power adaptor and cable: approximately 75 g

Colours
- Chalk, Charcoal, Coral. Aqua

Materials
- Durable fabric top
- External enclosure made from 20% post-consumer recycled plastic
- Non-skid silicone base

Supported audio formats
- HE-AAC, LC-AAC, MP3, Vorbis, WAV (LPCM), Opus, FLAC with support for high-resolution streams (24-bit/96 KHz)

Wireless
- Wi-Fi • Bluetooth® support
- 802.11b/g/n/ac (2.4 GHz/5 Ghz) Wi-Fi
- Chromecast and Chromecast Audio built-in
- Bluetooth® 4.1 input support

Sensors
- Capacitive touch

Speaker
- 360 sound with 40-mm driver

Mics
- 2-mic array
- Mic switch

Power
- 5 V, 1.8 A

Ports & Connectors
- Micro USB port

Operating system
- Android • iOS

Google Nest Hub

Key Features: See your life in one view and get things done hands-free. Google Nest Hub helps you make the most of moments at home. With Voice Match, get your calendar, commute, reminders and more right on the home screen, for example “Hey Google, show me my calendar. “ You can even get the news, make a shopping list and place calls to friends, family and local businesses. Voice-control compatible lights, cameras, TVs and more from a single dashboard.
Final Thoughts: Entry-level, video based addition to the collection.

Dimensions
- Depth: 67.3 mm (2.65”)
- Width: 178.5 mm (7.02”)
- Height: 118 mm (4.65”)
- Power cable: 1.5 m

Weight
- 480 g (16.9 oz)

Colours
- Sand, Aqua, Chalk, Charcoal

Display
- 177.8 mm (7”) LCD touch screen

Speaker
- Full-range speaker

Microphones
- 2-mic array

Sensors
- Capacitive touch

Connectivity
- Wi-Fi and Bluetooth® support
- 802.11b/g/n/ac (2.4 GHz/5 Ghz) Wi-Fi
- Bluetooth® 5.0 support

Power
- 15 W power adaptor

Ports
- DC power jack

Google Home

Key Features: Simplify your everyday life with the Google Home, a voice-activated speaker powered by the Google Assistant. Use voice commands to enjoy music, get answers from Google and manage everyday tasks. Google Home is compatible with Android and iOS operating systems, and can control compatible smart devices such as Chromecast or Nest.
Final Thoughts: Perfect for the first time user, features a host of abilities.

Dimensions
- Depth: 67.3 mm (2.65”)
- Width: 178.5 mm (7.02”)
- Height: 118 mm (4.65”)
- Power cable: 1.5 m

Weight
- 480 g (16.9 oz)

Colours
- Sand, Aqua, Chalk, Charcoal

Display
- 177.8 mm (7”) LCD touch screen

Speaker
- Full-range speaker

Microphones
- 2-mic array

Sensors
- Capacitive touch

Connectivity
- Wi-Fi and Bluetooth® support
- 802.11b/g/n/ac (2.4 GHz/5 Ghz) Wi-Fi
- Bluetooth® 5.0 support

Power
- 15 W power adaptor

Ports
- DC power jack

Operating system
- Android • iOS

Google Nest Mini

Key Features: Meet the second generation Nest Mini, the speaker you control with your voice. To play your favourite music from Spotify, YouTube Music and more, just say “Hey Google”. It sounds bigger and richer with 40 percent stronger bass than the original Mini. Ask your Google Assistant for help and get the best of Google – weather, news, or almost anything. Hear your personalised schedule, commute and reminders. Set timers and alarms and even turn on the lights. Nest Mini is compatible with hundreds of smart devices, such as lights, thermostats and TVs.
Final Thoughts: The latest and best version of the Google Home range.

Dimensions
- Diameter: 98 mm (3.85”)
- Height: 42 mm (1.65”)
- Power cable: 1.5 m

Weight
- Device: 181 g

Colours
- Colours, Chalk, Charcoal, Coral, Sky

Materials
- Durable fabric top made from 100% recycled plastic bottles External enclosure made with at least 35% post-consumer recycled plastic

Connectivity
- Wi-Fi • Bluetooth® support
- 802.11b/g/n/ac (2.4 GHz/5 GHz) Wi-Fi
- Bluetooth® 5.0
- Chromecast built-in

Power and ports
- 15 W power adaptor • DC power jack

Speakers
- Google Assistant built-in
- 360-degree sound with 40 mm driver

Mics
- 3 far-field microphones
- Voice Match technolog

Sensors
- Capacitive touch controls
- 3 far-field microphones

Processor
- Quad-core 64-bit ARM CPU 1.4 GHz
- High-performance ML hardware engine

Operating system
- Android • iOS

Google Nest Hub Max

Key Features: Make your smart home even smarter. Nest Hub Max works with hundreds of smart home devices, including lights, TVs and thermostats, allowing you to easily control them all from one place. You can also control compatible TVs, speakers and game consoles from Nest Hub Max with your voice or from the screen. Turn them on and off; control the volume, play, pause and search.
Final Thoughts: Adds video based features to the Google Home, a must!

Camera
- 6.5 megapixel camera with 127-degree wide field of view and auto-framing
- Face Match technology
- Quick Gestures
- Mic + camera switch

Dimensions
- Depth: 101.23 mm (3.99”)
- Width: 250.1 mm (9.85”)
- Height: 182.55 mm (7.19”)
- Power cable: 1.5 m

Weight
- 1.32 kg (2.91 lb.)

Colours
- Chalk, Charcoal

Display
- 10” HD touchscreen (1280x800)

Speakers and mic
- Stereo speaker system
- Google Assistant built-in
- Stereo speaker system (2 x 18 mm, 10 W tweeters, 1 x 75 mm, 30 W woofer)
- Far-field microphones
- Ultrasound sensing
- Voice Match technology

Sensors
- Ambient EQ light sensor

Connectivity
- Wi-Fi and Bluetooth support

Wi-Fi
- 802.11b/g/n/ac (2.4 GHz/5 GHz) Wi-Fi
- Bluetooth® 5.0 support
- Chromecast built-in
- 802.15.4 (at 2.4 GHz) thread support

Power
- 30 W power adaptor

Ports
- DC power jack

Operating system
- Android • iOS

Google Home First Time Setup

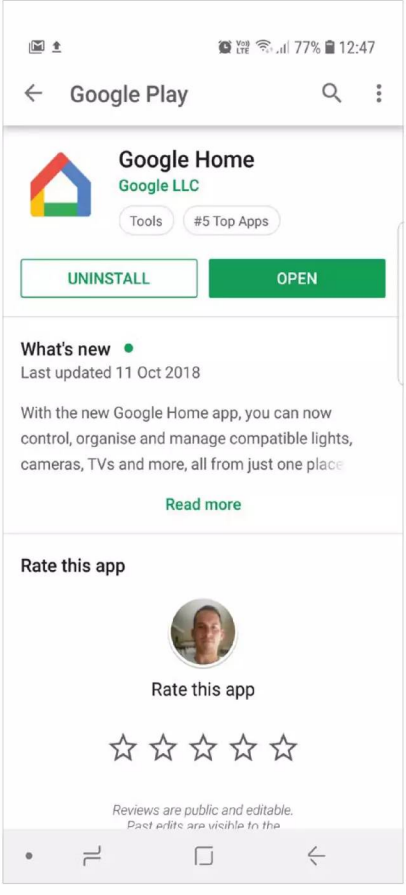
Setting up your Google Home device properly for the first time will make using it much easier, so take the time to get things right. You will need to have the speaker, an Android device, a Google account and a working Wi-Fi connection that both Android and Home devices can connect to.

Setting Up Google Home

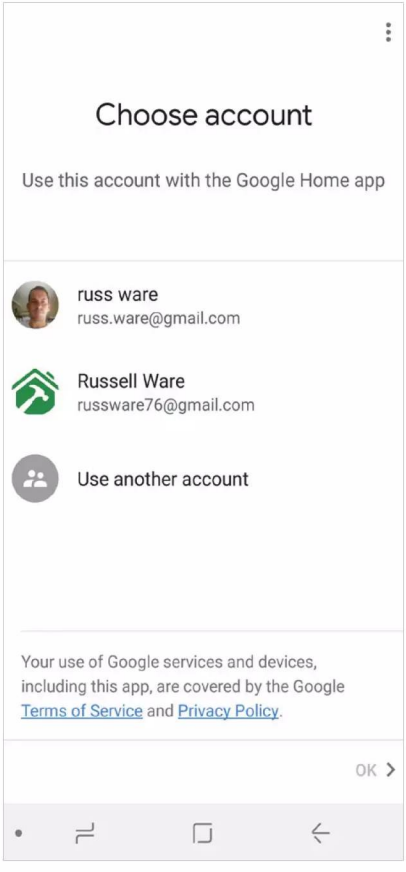
All of the setup for your Google Home speaker is done through the Google Home app for Android. Use this app for future access and changes to the settings.

STEP 1 Plug in your Google Home device and wait for the audio cue to show it is ready to be set up. Make sure that the switch that controls the microphone is set to "On". If you accidentally turn the microphone off on your speaker, the device will inform you accordingly.

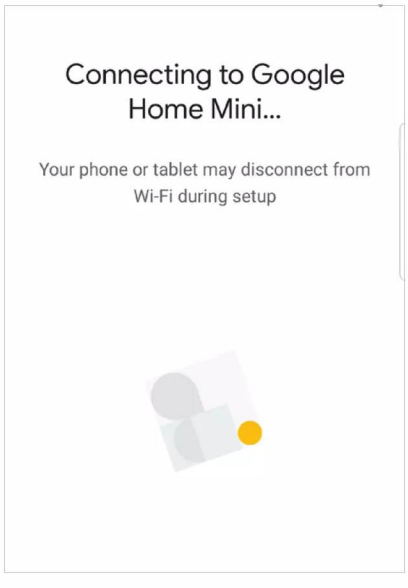
STEP 2 Currently, Google Home is only available for Android devices, and most have it pre-installed. If you don't already have it, find the app on the Google Play store, download and install it on your mobile device (phone or tablet). Once installed, open the app.



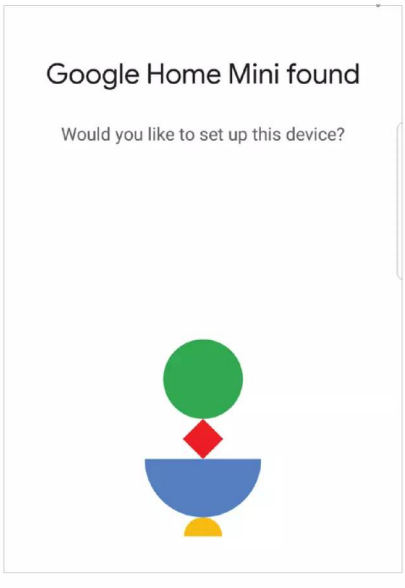
STEP 3 You will need to make sure that your mobile device is connected to the same Wi-Fi network you intend to use for the Google Home speaker. It won't work if you are using a 4G network to connect. Once connected, open the Home app and confirm which Google account you will use to log in.



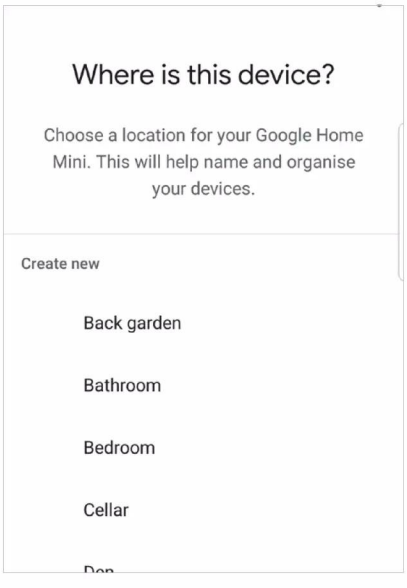
STEP 4 The Google Home app scans for nearby devices that are plugged in and ready to set up. If no devices are found, and you're setting up a device, tap Yes. Make sure that you're near the Google Home device that you're setting up and it's plugged into a wall socket. Then tap Next.



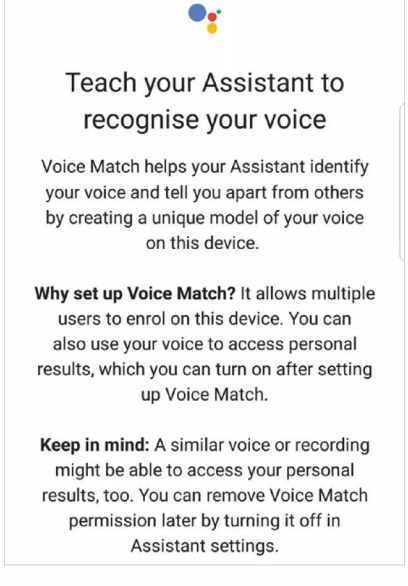
STEP 5 Hopefully your device will be found by the app, displayed on screen and you can then tap Next to continue. If you are setting up multiple devices, select the one you want to set up first, and then tap Next. The app will now connect your phone to your new Google Home ready for configuration.



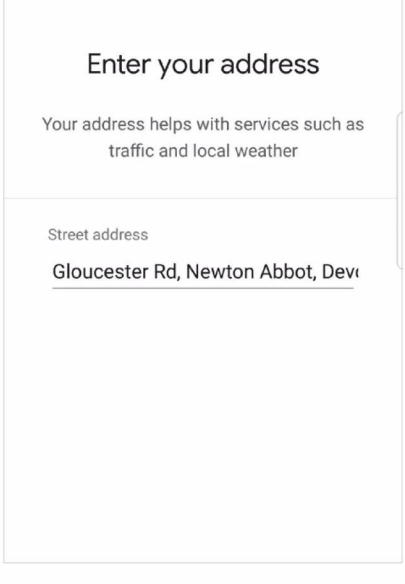
STEP 6 You should hear a sound on your speaker to show it is connected. You can now continue the setup by selecting the room it will be in (this is just to identify the speaker), choosing your region, and setting the assistant language you want to use. Once done, you will need to connect to your Wi-Fi network.



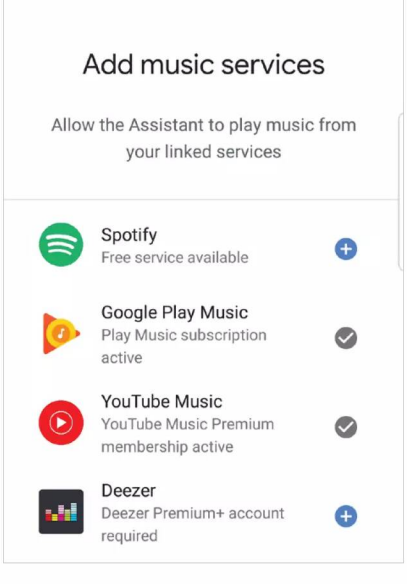
STEP 7 Next, to improve your Google Home experience, set up Voice Match. Voice Match allows multiple users to use the same device and get personalised results. Follow the prompts on screen to teach Google to recognise you. You can remove Voice Match settings later if you wish.



STEP 8 The Google Home app will ask for access to use your location to pre-fill your address. This is the address where your device is located. If you allow access, your address will be pre-filled; otherwise, you will need to enter it manually. When your address is entered tap Next.



STEP 9 You can now add your favourite services, for example music. Spotify, Google Play Music, YouTube Music and Deezer are just some of those available. If you add more than one, you will need to choose a default music service. Follow the further on-screen prompts to complete the setup.



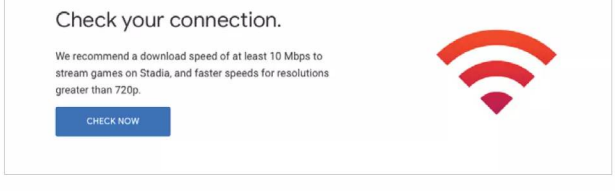
All About Google Stadia

With their Stadia project, Google hopes to revolutionise how we play games in the home and on the move. Their vision for the future is one where it is possible to play games on virtually any hardware without the need for expensive consoles or high-end desktops. Let's take a look at the hardware and explain how it works.

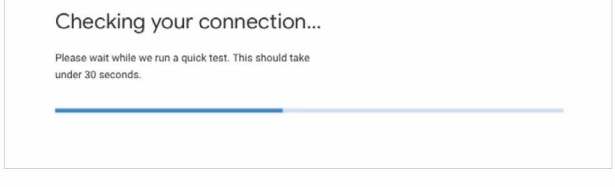
Stadia Speed Test

Before you begin your Stadia set-up, you need to ensure that your Internet connection is fast enough. Google has provided an online tool to do just that.

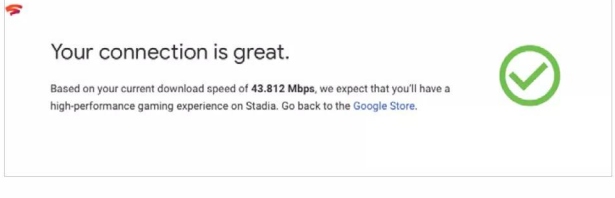
STEP 1 Open a web browser, preferably on the device with which you intend to use Stadia, and enter the following URL: projectstream.google.com Before you start testing your Wi-Fi speed you are advised to limit web traffic, such as downloads or streaming.



STEP 2 Once your Wi-Fi connection is free of other users, and clear of apps, tap the blue Check Now button on the left side of the web page. This activates the process, so you can simply sit back and wait for the results to appear.



STEP 3 When your Internet connection test is complete, it displays the results; this should take no longer than 30 seconds. These come in the form of a green tick for a pass and a red cross for a fail. A fail essentially rules out Stadia compatibility.



How Stadia Works

Google Stadia is a hardware-free, game streaming service that enables users to play a catalogue of game titles on a large variety of devices. All you need to play is the official Stadia joypad, a Chromecast, a screen and an Internet connection.

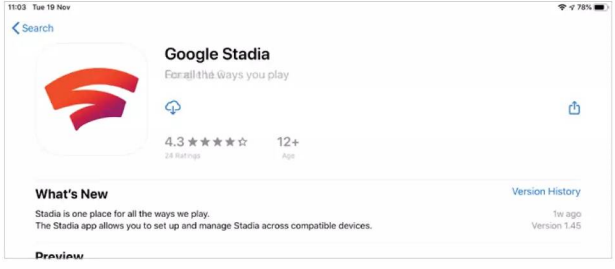
Stadia allows play on existing desktops/laptops computers, Smart TVs, tablets and smartphones. Play is enabled via the Stadia controller, which may indeed resemble a traditional joypad, yet is much more than that. Such unique features, exclusive to the joypad, include the ability to capture and share your gaming footage directly to YouTube.

So basically get your device online, connect your joypad and press play, that's it!

Getting Started with Stadia

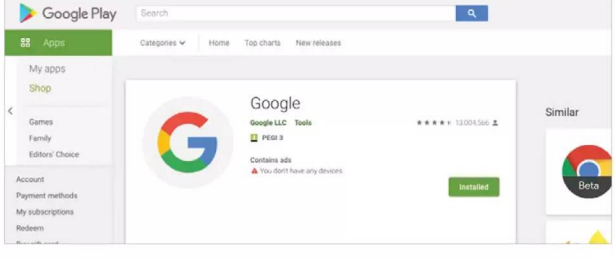
Are you ready to play some games? Let us take you through the set-up of your Google hardware with your monitor or TV so you can press Start with Stadia.

STEP 1 Using a mobile device (smartphone or tablet), you need to open the App Store on iOS, or Google Play on Android, and download the Stadia application. At this point, enter the invite code that was emailed to you at purchase.

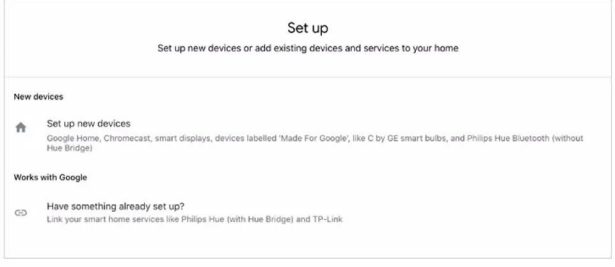


STEP 2 If you wish to use your Google Stadia on your TV, you need to set up your Google Chromecast Ultra first. NOTE: You need an Android or iOS mobile device to complete setting up Chromecast.

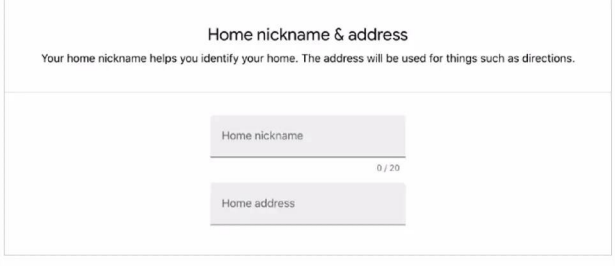
STEP 3 On your Android device, you need to download the latest build of the Google Home App. Sign in using your Google account and then connect the Chromecast to your TV via the HDMI input and USB for power.



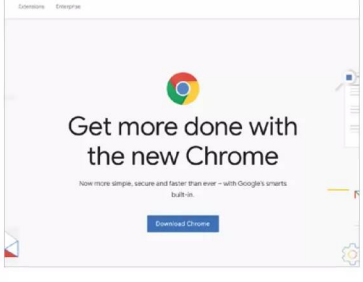
STEP 4 Ensure your Android mobile device connects to the same Wi-Fi network you want to link to your Chromecast Ultra. Open the Google Home app and, from the home screen, tap Add +>Set up device>Set up new devices.



STEP 5 Find your Chromecast Ultra from the list of new devices. Once selected, follow the instructions and the Google Home app pairs your device to your home network, thus enabling Stadia streaming via your Chromecast.



STEP 6 Finally, if you wish to play games on your desktop or laptop, you need to open a web browser on the video device you wish to use and visit: google.com/chrome and download the latest build of the Chrome browser.



What's in the Box?

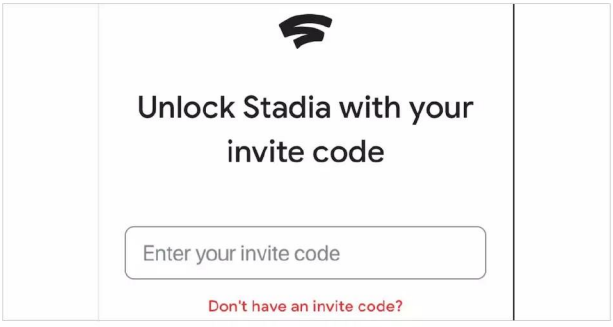
Having confirmed Wi-Fi compatibility, let's start unboxing your Google Stadia. Here's what's in store when you peel back the lid of your Stadia Premiere Edition.

- A Single Google Stadia Controller
- A Chromecast Ultra
- A Mains Charging Cable
- Three Months Subscription to Stadia Pro
- Documentation

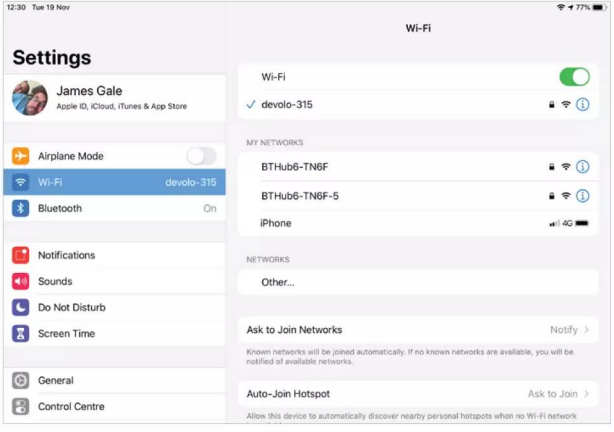
STEP 7 Now let's turn our attention to the Google Stadia Controller, once out of the box you need to ensure that your device is fully charged before you start setting up the controller itself.

STEP 8 Once the device is fully charged, unplug the power cable. Press the Stadia logo button on the controller for two seconds to turn it on. A vibration confirms that you have powered up the device.

STEP 9 Switching to your mobile device, open the Stadia app, using your invite code (if required), and tap the Controller icon to the top right, you may need to enable Location access first. Select your controller from the list of devices.



STEP 10 Your Stadia controller starts to vibrate to confirm connection and then, when prompted, tap Yes on the mobile app. Now tap Connect to your network using the same account as your mobile device.



STEP 11

You need to enter your Wi-Fi password and then tap Connect to Wi-Fi to complete the process. Your controller may automatically install an update, if it is required, and then you are ready to play.

Google Stadia Controller Controls Explained

With Stadia, the controller is the console, so understanding how this all-in-one device works is going to be essential to your gaming experience.

Understanding the Status Light

Blinking White:	Your controller is charged and ready to access your network via the linking code.
Solid White:	The controller is powered on, linked to a screen and ready for use.
Blinking Orange:	The controller needs connecting to a Wi-Fi network.
Solid Orange:	The controller is charging, when complete, the light turns off.

Capture and Share Footage

If you have a YouTube channel, or simply want to share your gameplay footage via social media, you can capture gaming using this button. Press once to take a screenshot or hold to capture video.

Stadia Official Specs

Weight:	268g
Dimensions:	163mm x 105mm x 65mm
Internals:	Custom 2.7GHz hyper-threaded x86 CPU with AVX2 SIMD and 9.5MB L2+L3 cache. 16GB of RAM with up to 484GB/s of performance. SSD cloud storage
Colours:	Clearly White, Just Black, Night Blue & Wasabi


WPS

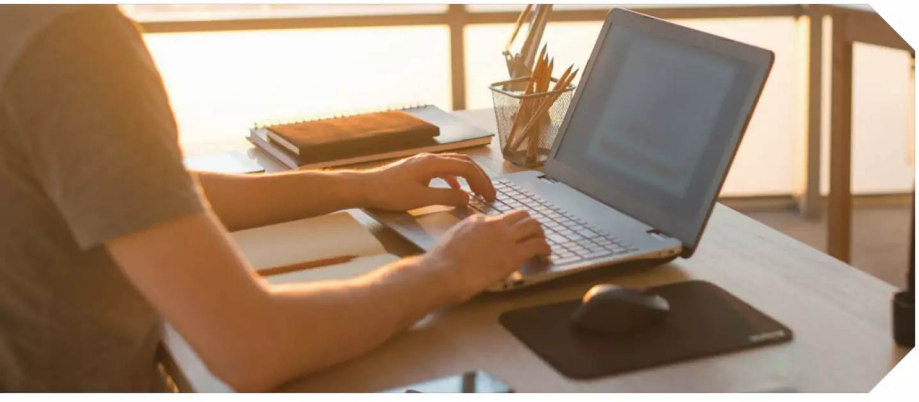
Combat Network Issues

There's a lot that can be done in the background to keep your network in order, and in this chapter you'll learn some of the best tools to help you combat network issues and performance lag. We look at some of the most used, and not so well known, commands for both Windows and Linux users, that can trace packets across the Internet, or just connect to an old school Bulletin Board Service.

There's also great troubleshooting tips, tricks and advice. Keep these pages handy, as they'll come in useful for those times when something on your network stops communicating with everything else.

Windows Networking Command Cheat Sheet

Windows contains numerous built-in commands for networking. These utilities and tools will help you discover problems with your network, as well as help you improve performance and monitor what's going on.

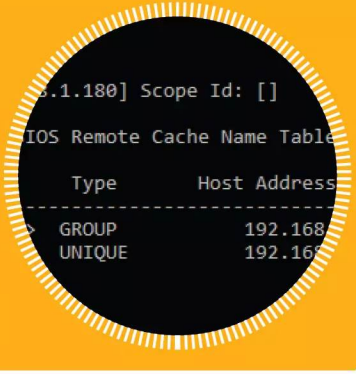


.: Telnet

This is a command that can be used to connect to another computer, or manage a router or switch. You can send and receive files, send commands and much more. With Telnet you're also able to connect to active Bulletin Board Systems. For example, enter: telnet bbs.balcos.net

.: NbtStat

The nbtstat command is a diagnostic tool for NetBIOS over TCP/IP. Its primary design is to help troubleshoot NetBIOS name resolution problems. It will display the human-friendly names of devices on the network along with their IP addresses.



.: Hostname :.

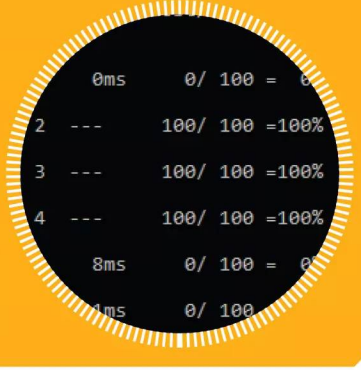
If you dicover that you are struggling to find the name of a Windows computer you've got on your network, simply enter the hostname command and it'll display the computer's local name.

.: Arp

Stands for Address Resolution Protocol and displays and modifies entries in the ARP cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses.

.: Pathping

This is a handy command that combines the best elements of Ping and Tracert. It will display the latency and packet loss between one computer and another (either locally or on the Internet), and after 300 seconds display a detailed report.



.: Ping :.

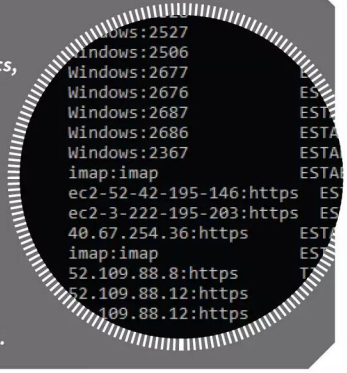
Ping is probably the most familiar of networking command line tools. With it you're able to send an echo request to a device locally, or on the Internet, and receive a reply.

.: Ipconfig

Probably one of the most used networking commands in Windows. Ipconfig will display information on the local computer's network interfaces, such as IP addresses (both IPv4 and IPv6), Hostname, gateway and so on.

.: Netstat

Stands for Network Statistics, this command will display connection information, routing tables and so on. Entering the command will display what's going on while you use the network and Internet. Use netstat -e for interface stats.

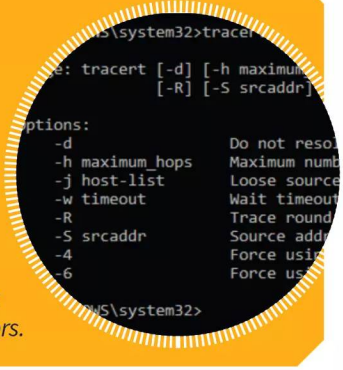


.: Netsh :.

This is a complex command that, when entered, will put you into a different shell, the Network Shell (netsh). It's capable of displaying and configuring information regarding a computer's networking setup.

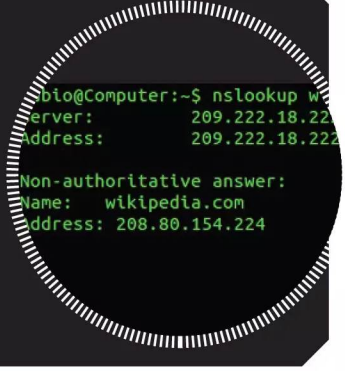
.: Tracert

Stands for Trace Route will examine the path to a remote computer, either locally or on the Internet. For example, entering tracert google.com will display the hops taken over networking devices to get to one of the Google servers.



.: Nslookup

This tool can be used to look up and diagnose the Domain Name System (DNS), of a location on the local network or Internet.



.: Getmac

Every network interface has a unique Media Access Code assigned to it. Some routers are able to limit connection to the network by only allowing user-entered MAC addresses in. You can get the MAC address of a Windows computer by entering getmac.

.: Route :.

The Windows Route command allows you to view the device's routing tables. To do so, simply type Route Print. This will print the network interfaces, IPv4 and IPv6 route tables.

Linux Networking Command Cheat Sheet

Linux has many networking commands available to it. Some are built in to the OS, whereas others will need to be installed; but all are great in their own special way.

.: HTTPie

This is a single HTTP command that's designed for debugging and interaction with HTTP servers and other web services. There's lots of support, and it features a great looking UI.

.: Ping

One of the most used networking commands for troubleshooting and testing network connectivity. Ping works by sending Echo Request packets to a user-specified IP destination, and waits for a reply.

.: Wget :.

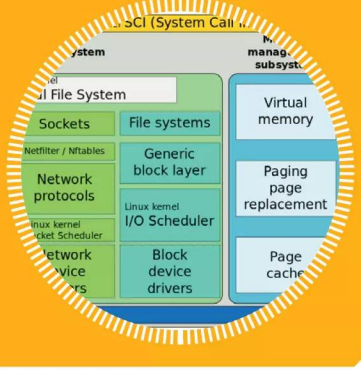
This is a handy command that combines the best elements of Ping and Tracert. It will display the latency and packet loss between one computer and another (either locally or on the Internet), and after 300 seconds display a detailed report.

.: cURL :.

cURLStands for Client URL, and transfers data to or from a network server using one of many supported protocols. It's perfect for shell scripts, as it can be used without user interaction.

.: Tc

Is used to configure traffic control, such as limiting the bandwidth use of a particular service to simulate Internet connections.



.: Ifconfig :.

Stands for Interface Configuration, and is used to display and configure the local network adapter. With ifconfig, you're able to view a computer's IP address, gateway and so on. Can also be used to setup a network port.

.: Whois

The whois command is able to process and display information about a user-specified domain name. For example, enter: whois google.com, for information on the Google.com domain.

.: Route

This command is used to show and manipulate the IP routing table for a Linux computer. With it you can setup static routes to specific hosts or networks.

.: Traceroute :.

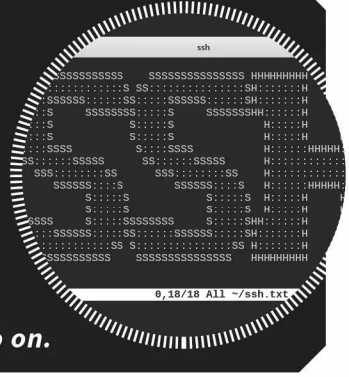
A tool used to diagnose and display the route of packets to and from user specified locations. It's great for finding slow areas of a network, so you can tweak any network extenders that the packets hit on their way to the location.

.: Nload

Can help you keep an eye on your network traffic and bandwidth usage in real time. It monitors incoming and outgoing traffic, using graphs, and provides additional information on the total transferred data and network use.

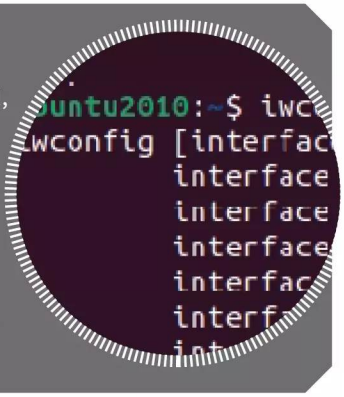
.: SSH

Provides a secure, encrypted connection between two devices on a network. With it, you can connect to other computers and run commands, transfer files and so on.



.: Iwconfig

Like the ifconfig command, but iwconfig is exclusively designed to work with wireless network interfaces. You can set parameters, such as SSID, frequency and so on.



.: Tcpdump :.

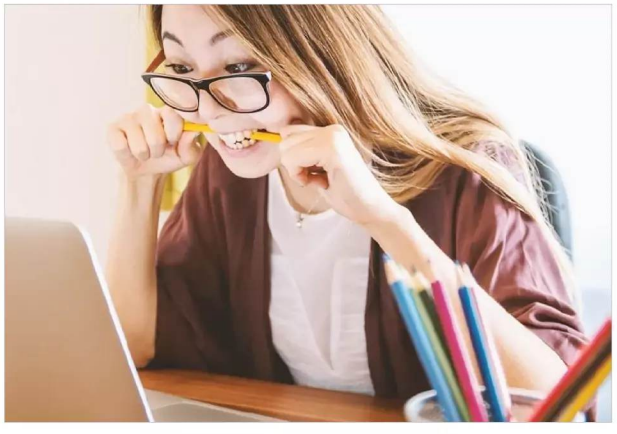
A famous networking tool that's a packet analyser to display TCP/IP and other network packets that are being transmitted to and from a Linux computer.

Troubleshooting Your Wi-Fi Network

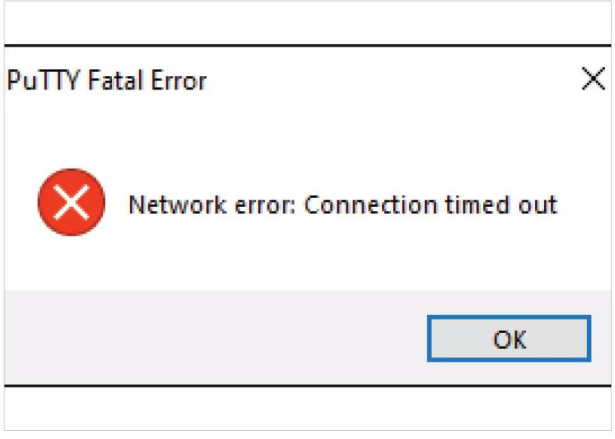
Wired networks are often a lot more sturdy compared to a wireless network, but they're not bulletproof. Thankfully, problems can easily be fixed, so here are our top ten troubleshooting tips for solving wired network issues.

TIP 1 **SLOW OR NO ACCESS IN SOME ROOMS –** There's a good chance that the room in question has become a bit of Wi-Fi dead zone. Load up a network analyser and check the signal output in the room in question. If needs be, reboot any network extenders and the router.

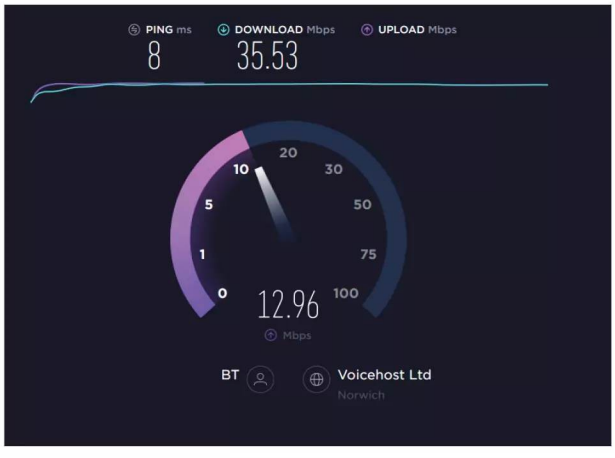
TIP 2 **SLOW INTERNET –** This could be one of two things: a problem with the router and your network, or a problem with the ISP. Test the connection by directly plugging a device into the router's Ethernet ports. If the problem persists, then call your ISP. If it's okay, then turn off all your networking equipment and one-by-one power them up, while testing to find the culprit.



TIP 3 **REFUSAL TO CONNECT –** Occasionally, there's a device that will refuse to establish a connection with your wireless network. First thing to try is a physical Ethernet connection (if it has one). If it works, try re-installing the Wi-Fi drivers on the device. If that's not possible, try another Wi-Fi network; it could be a problem with the device's Wi-Fi card.



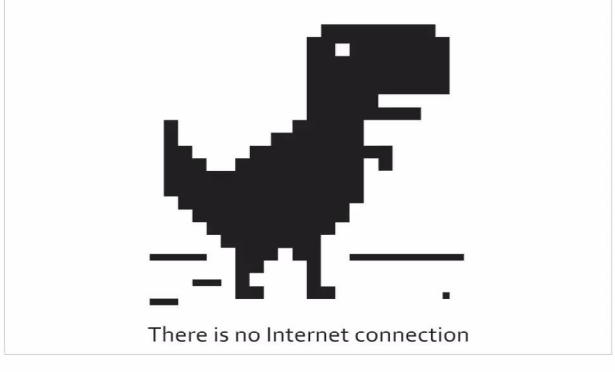
TIP 4 **RANDOM LOSS OF BANDWIDTH –** First check is to establish a pattern. Does it happen when you power on something else in the house, if so, it could be causing interference with the signal. Does it happen when a certain device is connected? Check the device, as it could be downloading a huge file, or it could have some form of malware.



TIP 5 **UNKNOWN DEVICE DISCOVERED –** If you maintain an orderly network, and you've just spotted an unknown device on your network, then you need to act quickly. If possible, drop the connection via the router's web interface, then change your access password. Check all devices for malware, ask other family members if they know who it could be. Worst case, change all passwords.

TIP 6 **WI-FI IS COMPLETELY GONE –** If nothing is connecting to your Wi-Fi, then the problem is likely with your router. Check the router, if you can access its web interface, and check the access logs and check for any recent updates (an update from the ISP could have damaged it). If a reboot doesn't fix it, contact your ISP.

TIP 7 **EVERYTHING WORKS, BUT NO INTERNET –** Check the indicator lights on the router, if the Internet LED is off, then reboot the router and wait for a connection. If the LED is on, but still no Internet, try installing a VPN and seeing if you can connect; it could be an issue with the ISP's DNS entries.



TIP 8 **FORGOT THE WI-FI PASSWORD –** If you've forgotten your Wi-Fi password, then you may need to factory reset the router. Use a paperclip and locate the tiny pin-hole (usually marked Reset). Poke the paperclip in for 30 seconds. Reboot the router. It should be reset back to its original settings and password.

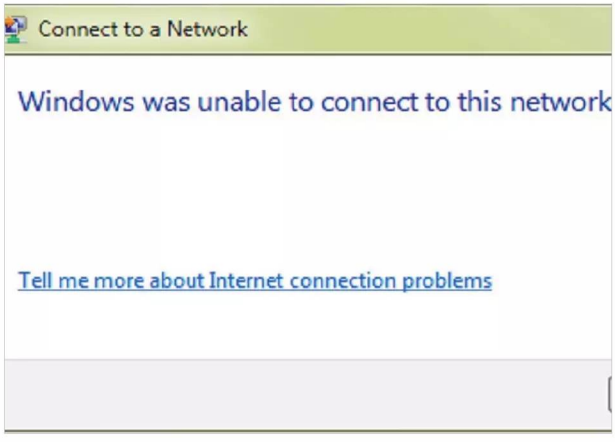
TIP 9 **OVERALL POOR SIGNAL –** Providing your router is working well, check with a wireless device while standing next to the router. If it's okay, then the problem is likely a poor signal spread. Try and reposition the router, but don't put it in a cupboard, and see if that helps. If the signal is poor while next to it, there could be a problem. Try rebooting, otherwise contact your ISP.

TIP 10 **SPEEDS AREN'T AS ADVERTISED –** If your network extender or router isn't performing at the speeds it was advertised as, try the following. Ensure that the router's configuration is setup for maximum signal strength. If it has external antennae, move them around to change the signal spread. Reboot the router and any Wi-Fi extenders. Reposition the router and extenders for a better signal through walls and such.

Troubleshooting Your Wired Network

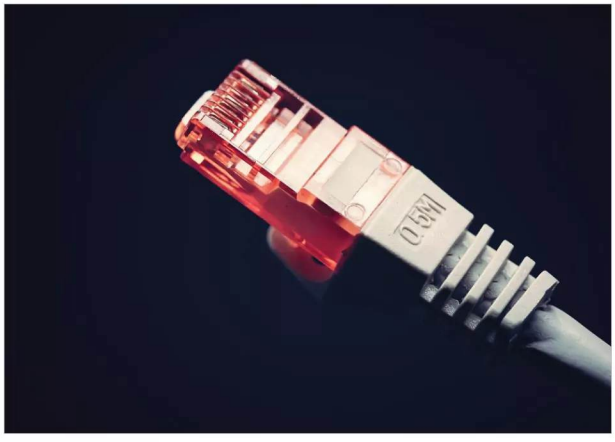
Wired networks are often a lot more sturdy compared to a wireless network, but they're not bulletproof. Thankfully, problems can easily be fixed, so here are our top ten troubleshooting tips for solving wired network issues.

TIP 1 **NO CONNECTION (ONE PC) –** If your computer is reporting no connection, it's time to get behind the machine and double-check the Ethernet port. Check that the cable is fully inserted, as they can get caught by feet and pulled slightly. Check the cable end isn't damaged. If there's still no connection, check other machines (a router reboot may be needed).



TIP 2 **NO CONNECTION (ALL PCS) –** If all your computers and other devices aren't connecting, check any switches that they're connected to. Switch plugs, and even powerline adapters, can blow a fuse. Check your router's switch connection LED is lit up, if not try a different port. If all else fails, try direct connection to the router, as it could be faulty.

TIP 3 **CONNECTION KEEPS DROPPING –** One of the main reasons as to why wired connections keep dropping is a damaged, or poorly created network cable end. Check the cable with a cable tester, check the ends by giving them a pull. If they're loose, or the cable test fails, then replace the ends or the cable itself.



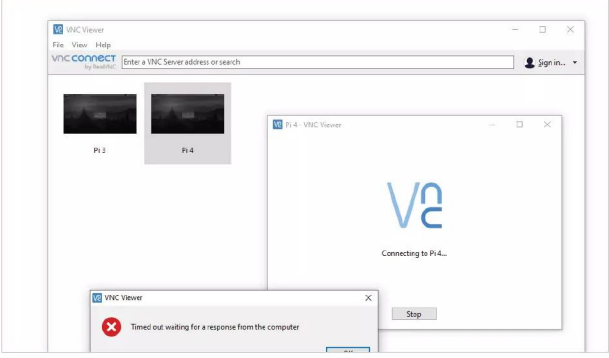
TIP 4 **POOR SPEEDS –** A main culprit of poor wired network speeds is the cable is too long. If the cable is over 100 metres (300 ft), then the signal will begin to drop significantly. If your cable is coiled up behind furniture, or in the loft space, try to shorten its length and check the connection speed.

TIP 5 **POOR CONNECTION, OR NO CONNECTION, BETWEEN POWERLINE ADAPTERS –** Often powerline adapters will lose their connection with each other. When this happens, power off both adapters, then power up one and after a few seconds power up the other. Wait for a few more seconds to see if the connection is okay. If it fails, try pin-hole resetting the adapters.

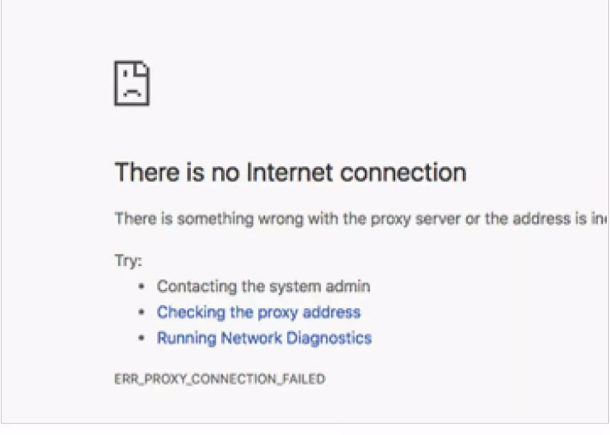
TIP 6 **POWERLINE ADAPTERS WON'T PAIR –** Sometimes powerline adapters won't pair with each other if there is already a set of powerline adapters already on the network. Turn off the existing powerline adapters, then power up the new pair. After a connection has been made, power up the existing pair.

TIP 7 **SOME PORTS ON A SWITCH CONNECT SLOW –** If you discover that some of the ports on your switch appear to be operating at 100Mb/s instead of 1Gb/s, then check the following. Ensure that device connected to the port has a 1Gb/s Ethernet port (some smart TVs don't). Check that the switch has more than one 1Gb/s port – some are 100Mb/s with a 1Gb/s uplink port.

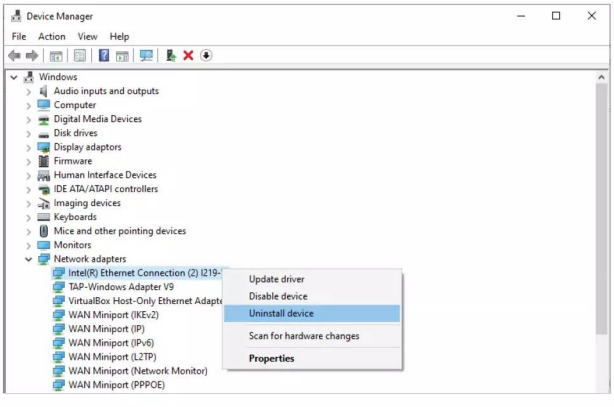
TIP 8 **CAN'T CONNECT TO ANOTHER PC –** If you're unable to connect to another PC on your network, check both connections to the router, on both PCs. Also, check that the PC you're connecting to isn't blocking your connection via the firewall.

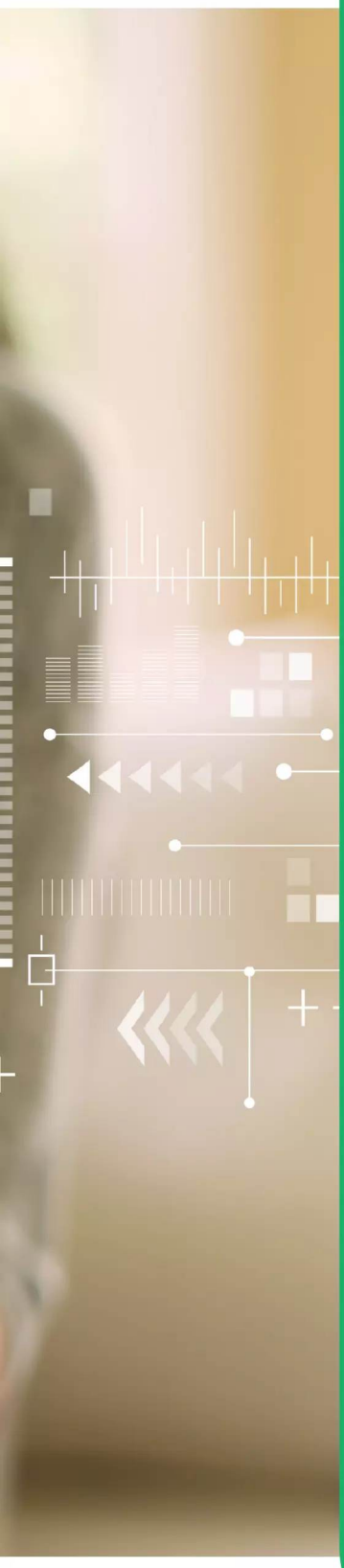


TIP 9 **NO INTERNET CONNECTION –** No Internet connection usually means there's something going on with the router, so that should be your first port of call. Check the router's LEDs, if the Internet is off, try and reboot, otherwise use a phone to check the status of the ISP's services.



TIP 10 **PC WON'T CONNECT VIA ETHERNET –** This could be one of several things. First check the cable going into the Ethernet port; use a different cable if necessary. Check the drivers by opening Device Manager and locating the network device. Right-click and select Update Driver. Also, try Uninstall Device, then Search for New Devices.





How To Protect Yourself

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

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

Types of Security Risk

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

Here Be Dragons

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

01 Viruses

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

02 Ransomware

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

03 Worms

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

04 Trojans

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

05 Spyware

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

06

Adware

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

07

Hacking

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

08

Social Engineering

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

09

Phishing

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

10

Rootkits

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

Hackers and You

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

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

> ***"You've been hacked!"***

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

Monetary Motivation

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

Personal Information

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

Parasitic Infection

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

Exploitation

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

Stealing Bandwidth

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

Access to Your Webcam

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

Access to Your Microphone

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

Zombie Apocalypse

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

Cyber Vandalism

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

Distributing Illegal Material

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

The Virus Top Ten

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

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

> ***Digital Destruction***

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

1 Storm Worm

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

2 Conficker

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

3 Daprosy Worm

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

4 Stuxnet

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

5 Duqu

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

6 Shamoon

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

7 CryptoLocker

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

8 Regin

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

9 Rombertik's Endless Loop

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

10 Tiny Banker

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

Be Smart

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

Weakest Links

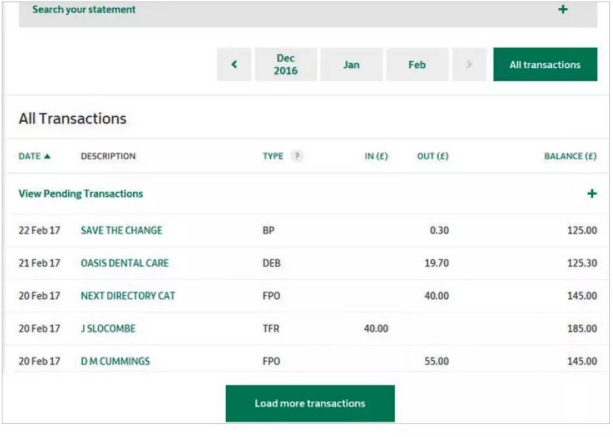
In terms of digital security, you're only as strong as the weakest link in your security chain. You can tick all the security boxes but if you don't know what to look for in the first place you're still vulnerable.

PASSWORD CHANGE

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

BANK ACTIVITY

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

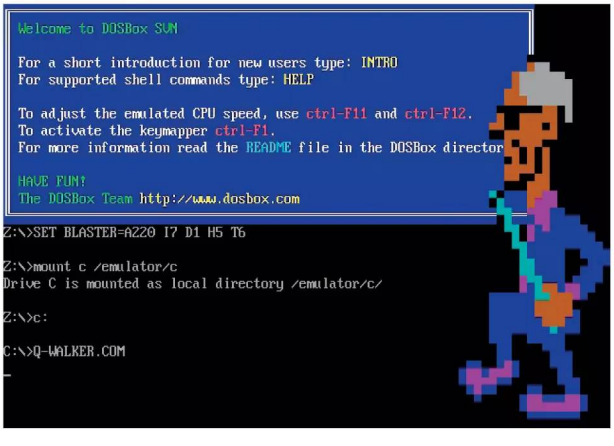


PERSONAL SPAM

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

SLOW PC

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



SLOW BROWSER

In relation to the previous tip, a browser slow down can also indicate that something is potentially going on. Browser hijacking can adversely affect the speed at which pages load, as it's sending information to a remote source. Naturally it's not always a digital security issue but to make sure, check your system.

POP-UPS

Furthering the browser issue, if you suddenly notice a lot more advertising, pop-ups or similar, then it's usually a good sign that you're infected with some form of adware or Trojan tracker.

INFECTED CONTENT

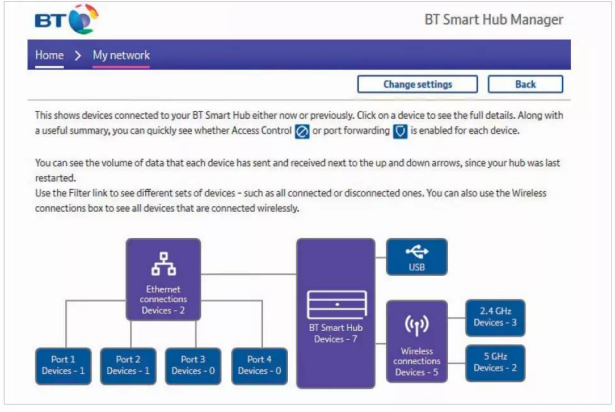
Viruses want to be spread from one computer to another and they can infect your email or social media platforms. If you suddenly have your friends asking you why you're posting adverts for pharmaceutical enhancements, then there's a good chance you're infected with something.

RANSOMWARE WARNING

In the case of a ransomware attack, you don't often get much warning that something is about to happen. Generally speaking, a sudden and inexorable slowing down of your computer will be a key element, as the ransomware is frantically encrypting your files in the background.

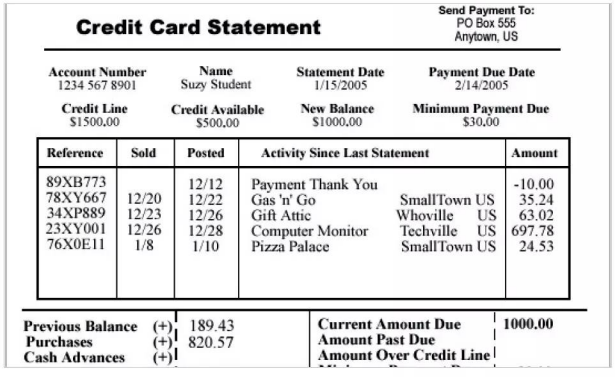
ROUTER LOGS

It's always recommended to check your router's logs frequently. Although hackers are generally anonymous groups or individuals on the other side of the world, often a hacker could simply be a neighbour leeching your broadband connection. Check the logs for any unidentifiable computers attaching to the router.



BANK STATEMENTS

Keeping an eye on your credit card statements will reveal any compromising security leaks. Just as with bank statements, small transactions are usually the first indicator, then once the hacker knows the card is valid they can then blitz it until you've run up a huge debt. Always check your statements and mark any suspicious transactions.



Credit Card Statement

Send Payment To:
PO Box 555
Anytown, US

Account Number	Name	Statement Date	Payment Due Date
1234 567 8901	Suzy Student	1/15/2005	2/14/2005

Credit Line	Credit Available	New Balance	Minimum Payment Due
$1500.00	$500.00	$1000.00	$30.00

Reference	Sold	Posted	Activity Since Last Statement		Amount
89XB773		12/12	Payment Thank You		-10.00
78XY667	12/20	12/22	Gas 'n' Go	SmallTown US	35.24
34XP889	12/23	12/26	Gift Attic	Whoville US	63.02
23XY001	12/26	12/28	Computer Monitor	Techville US	697.78
76X0E11	1/8	1/10	Pizza Palace	SmallTown US	24.53

Previous Balance	(+)	189.43	Current Amount Due	1000.00
Purchases	(+)	820.57	Amount Past Due	
Cash Advances	(+)		Amount Over Credit Line	

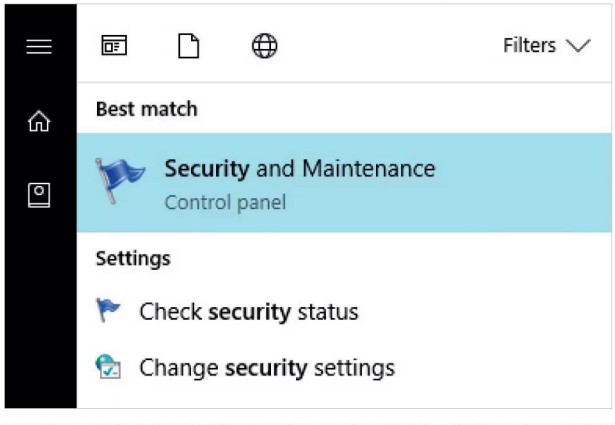
Setting Up Windows Security

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

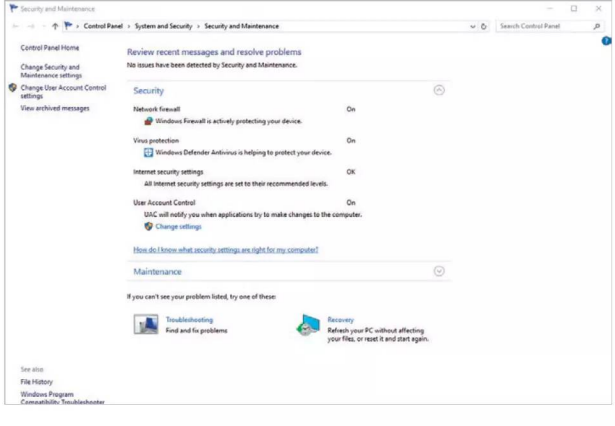
Are You Secure?

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

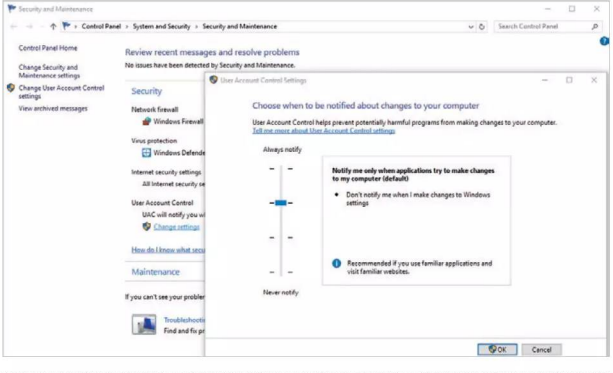
STEP 1 Start by clicking on the Windows Start Button or pressing the Windows key on your keyboard. Enter security into the search bar and click the first option that appears in the results, Security and Maintenance.



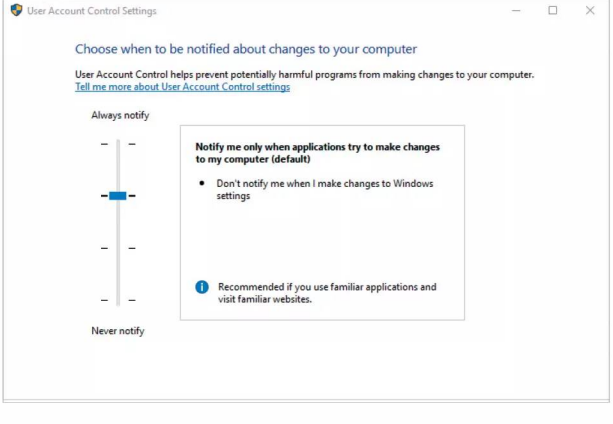
STEP 2 This will open the Security and Maintenance section of the Control Panel. There are two main sections within this page, click on the Security section to expand it. Ideally all the options within the Security section should be displaying On, with the exception of Internet Security Settings which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



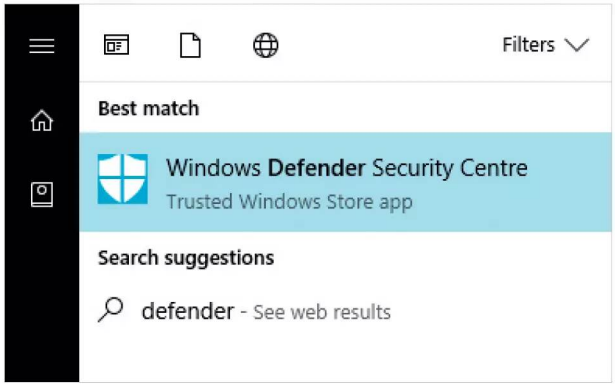
STEP 3 Should any of the options display No, then you'll need to check the setting relating to that particular feature. For example, if your User Account Control (UAC) is set to Off, click the Change Settings link under the UAC option. The other features can be found via a search from the Windows Start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



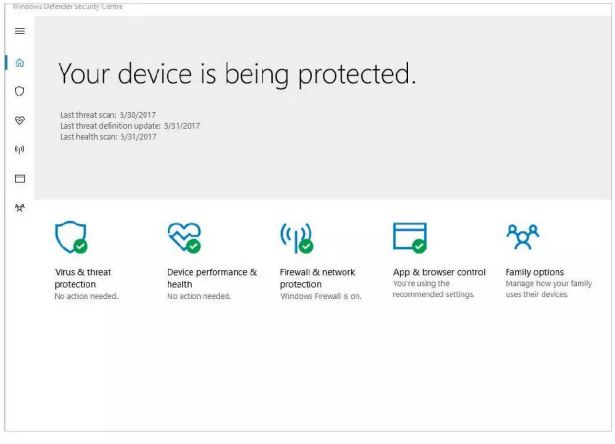
STEP 4 UAC will warn you of any attempt to access a system critical file. If any malware wants to alter a file, then you're asked if you want to proceed; obviously you don't, so you can say no and investigate the issue. There are various settings to choose from but the second step down from the top is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



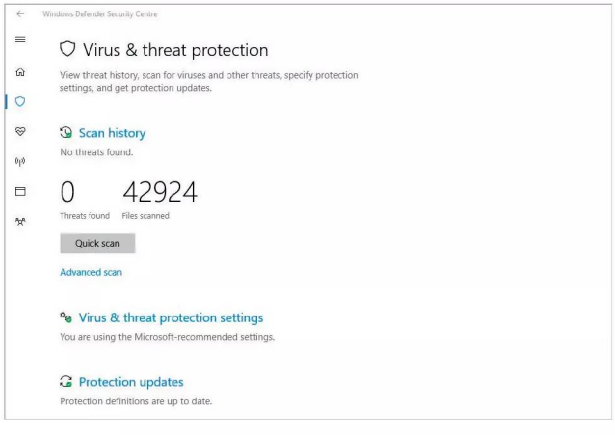
STEP 5 Close down the Security and Maintenance window, then click the Windows Start Button and search for Defender. Click the resulting Windows Defender Security Centre option.



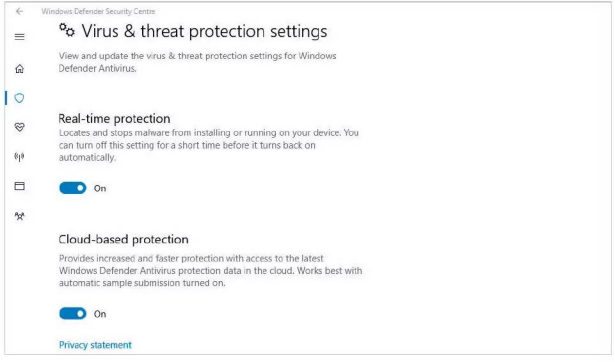
STEP 6 If you're not using a third-party security and AV suite, then you need to make sure that Windows Defender is activated and working. There are numerous options available in the new-look Creators Edition Windows update of Defender. Each can be selected with a mouse click and viewed separately.



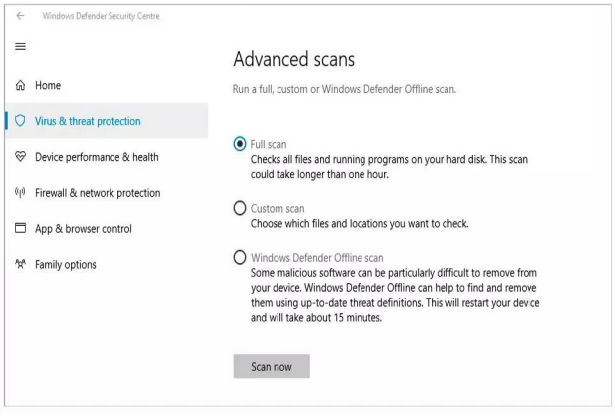
STEP 7 Click the Virus & Threat Protection option. This will open a new window allowing you to perform a Quick or Full Scan of the system that details the number of threats found and the number of files scanned.



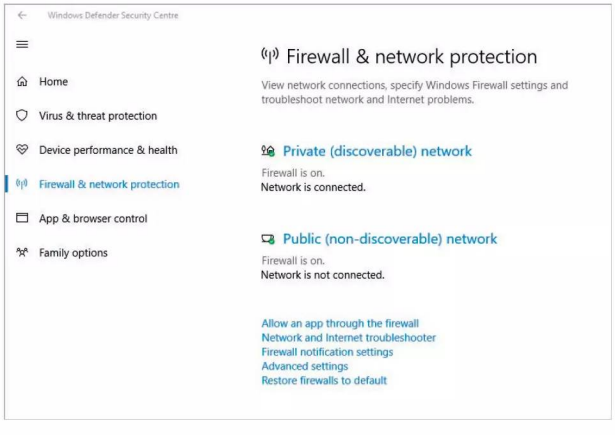
STEP 8 If you click the Virus & Threat Protection Settings option, you can further opt to improve the system protection. Make sure that all the sub-options are set to On and scroll down to define the program's default Notifications.



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



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



Why Updating is Important

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

Update, reboot, update, reboot

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

PATCH VULNERABILITIES

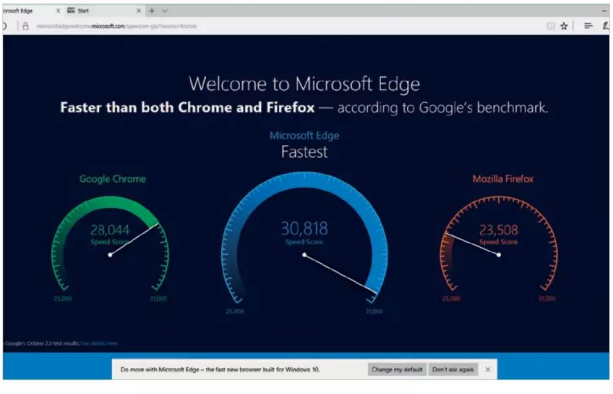
Windows updates patch recognised security holes in the core system. Many of the viruses around today exploit a vulnerability in the Windows code that hasn't been fixed yet. So when an update comes along, that potential flaw will be ironed out.

EXTRA SECURITY

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

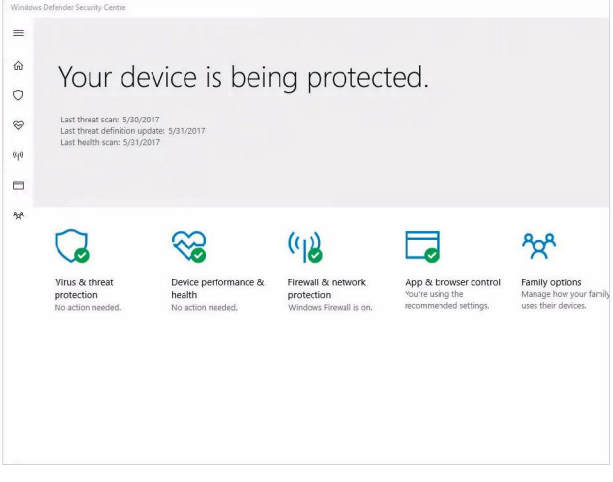
BROWSER UPDATES

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



DEFENDER UPDATES

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

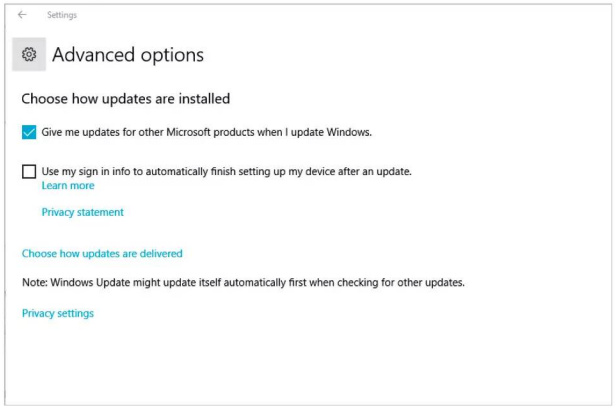


FIREWALL UPDATES

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

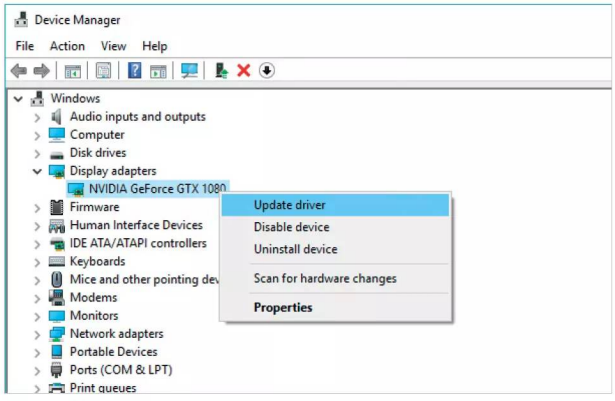
OFFICE PATCHING

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



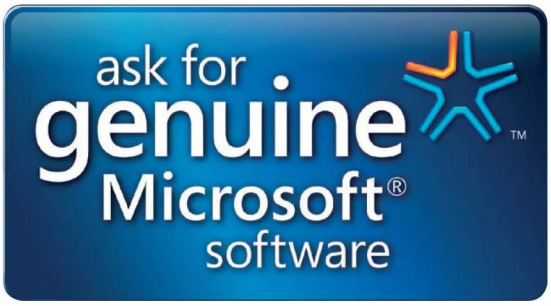
SIGNED DRIVERS

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



GENUINE SOFTWARE

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

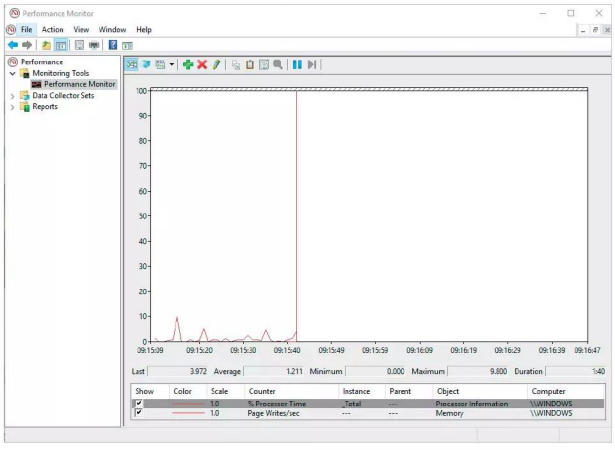


FUTURE UPDATING

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

STREAMLINING CODE

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



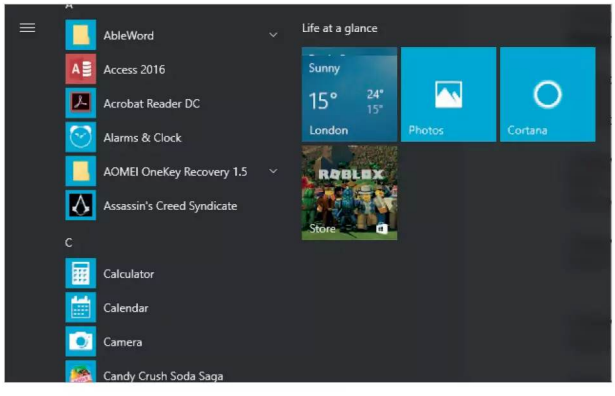
What to Keep Updated and How

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

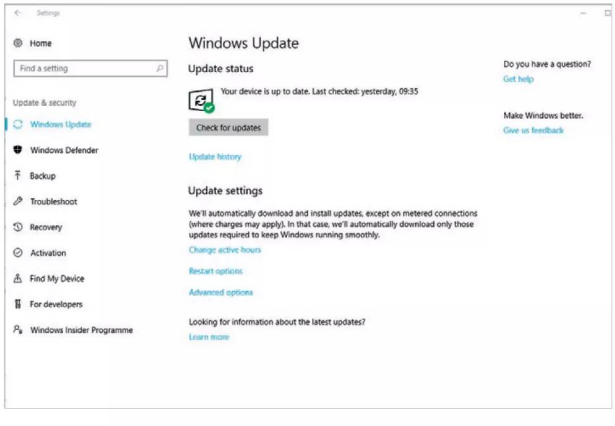
Keeping Up To Date

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

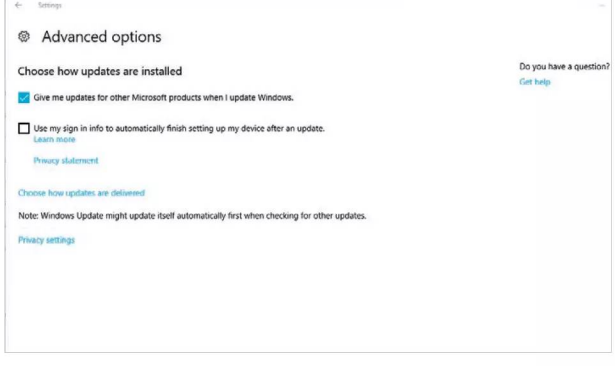
STEP 1 The first port of call is undoubtedly Windows Update. Click on the Windows Start button followed by Settings, the cog icon just above the power icon on the strip to the side. This will open the Windows Settings interface, locate the last entry, Update & Security and click it.



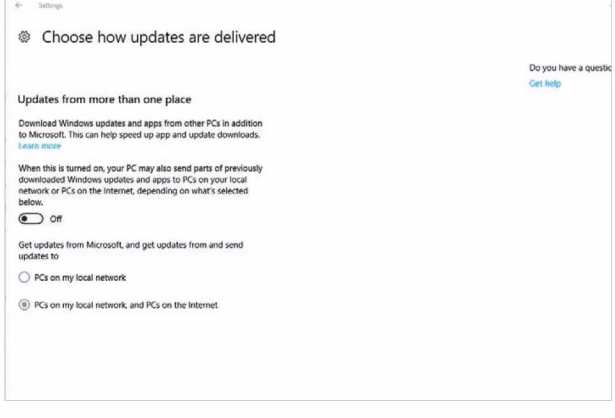
STEP 2 By default Windows Update will automatically check for, download and install updates for the core Windows files. You can check for any on the spot by clicking the Check for updates button; and you can see what's already been updated by clicking the Update history link under the update button.



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

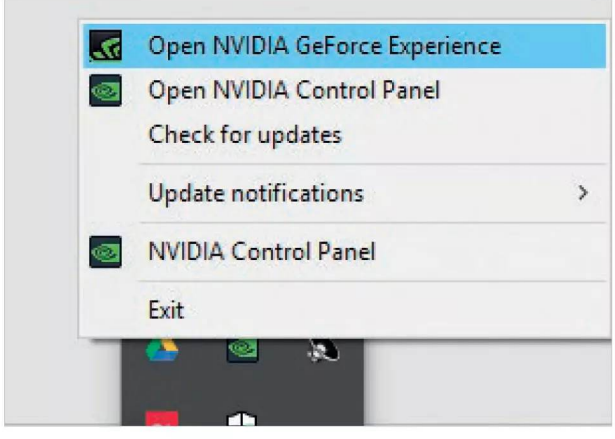


STEP 4 Within the Advanced Options page click the link for Choose how updates are delivered. This page details the way Windows updates can be pushed to other computers on your network, or even the Internet. Whilst it's a grand idea, there are concerns over privacy from some factors of the community.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

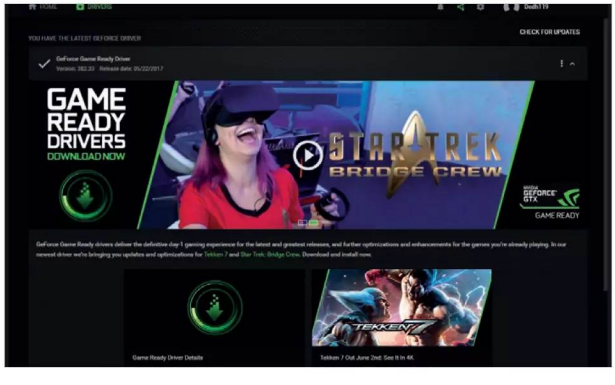


STEP 5 Hardware drivers are usually automatically updated by Windows Update but whilst signed by Microsoft the drivers themselves aren't always the latest versions. Therein lies a problem: even though signed, the MS drivers won't utilise the hardware as well as the driver developed by the hardware manufacturer.

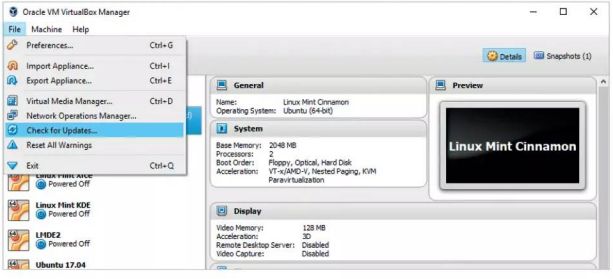
STEP 6 In such cases it's often best to use the hardware manufacturer's driver, as this is more up to date and features security patches as well as performance updates. For example, if you own an Nvidia graphics card right-click the Nvidia icon in the taskbar and select Open Nvidia GeForce Experience.



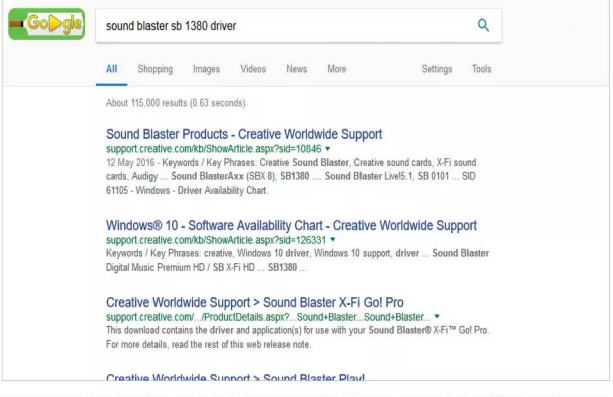
STEP 7 The Nvidia GeForce Experience allows you to improve in-game graphics and check for the latest drivers. Usually this is done automatically, and you are notified of any available drivers. However, If you want to check manually, click on the Drivers tab followed by Check for Updates.



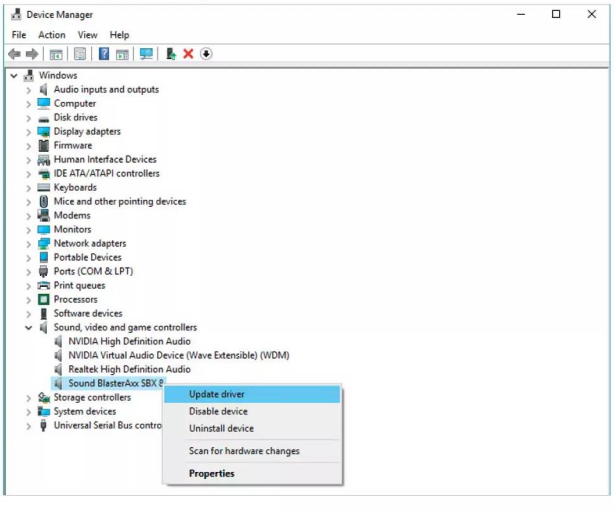
STEP 8 Third-party programs and applications also require regular update checks. Again, this is usually done automatically; when you launch the program in question it often checks for the latest version. If not, look for links such as Check for Updates or similar, usually in the Help, About or even under the File menus of your favourite app.



STEP 9 If you've attached some hardware and Windows hasn't been able to load a driver for it, and there isn't any documentation detailing the driver (this often happens with hardware purchased from eBay and the like), then you'll need to hunt one down. Start by locating the device's product name and number and enter it into a search engine.



STEP 10 You can often force Windows to locate a driver by right-clicking the Windows Start button and choosing Device Manager from the menu. In the Device Manager window, select the hardware you want updating, right-click it and select Update Driver.



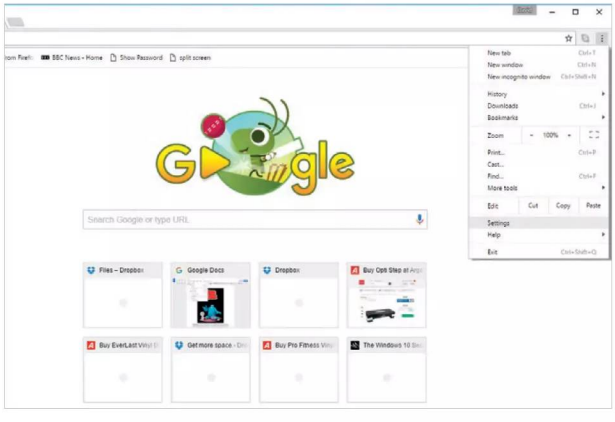
How to Secure Your Web Browser

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

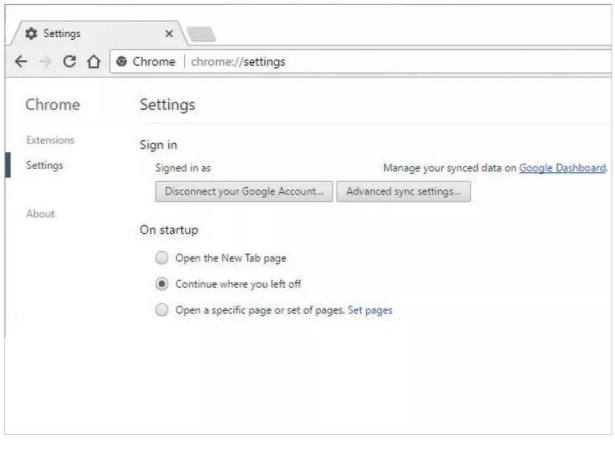
Safer Surfing

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

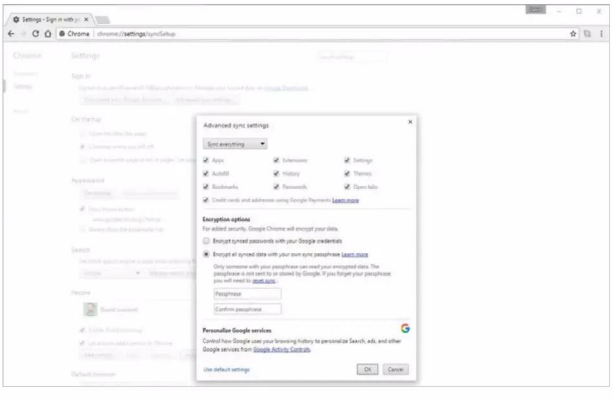
STEP 1 Start by opening Chrome and clicking on the three vertical dots in the top right of the browser window. This is the link to the available options; from the list choose Settings.



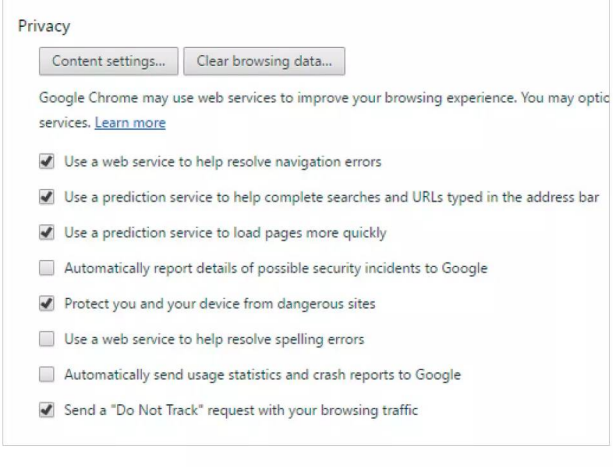
STEP 2 It's generally recommended that you sign into Chrome using a Google account, as this can greatly improve the overall security of the browser. For example, when you sign in, under the Sign In section in Settings, click on the Advanced Sync Settings button, the first option available.



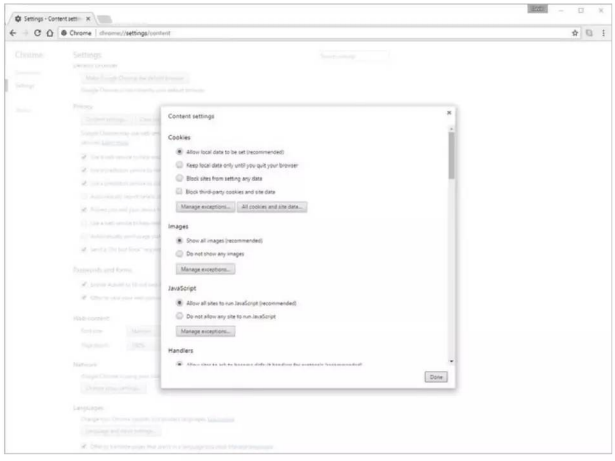
STEP 3 With the Advanced Sync Settings box open, select the option for Encrypt all synced data with your own sync passphrase. Enter a secure passphrase you can remember in the boxes provided and this will enhance the security of all data synced between Chrome and the Internet.



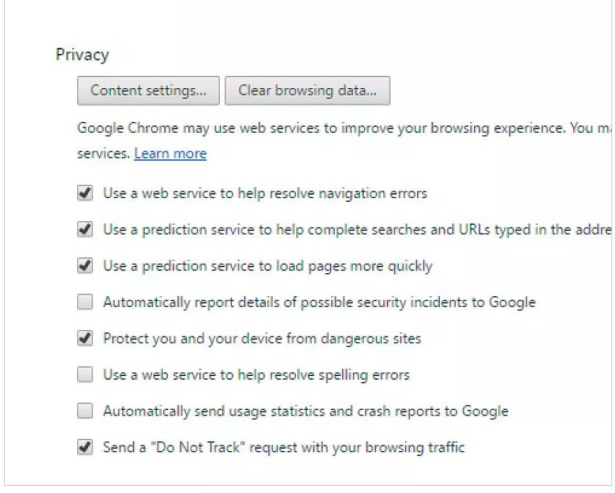
STEP 4 Look to the bottom of the Settings page and click the link for Show Advanced Settings. The first new section to appear under the Advanced settings is Privacy. Start by clicking on the Content Settings button.



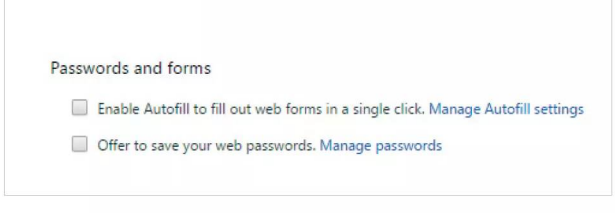
STEP 5 Content Settings allows a greater degree of control over Cookies, JavaScript, Flash, Pop-ups, your computer's microphone and even the webcam. It's an extensive list so we can't go into all the options within this limited space. For maximum security, disable JavaScript and Flash and make sure the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



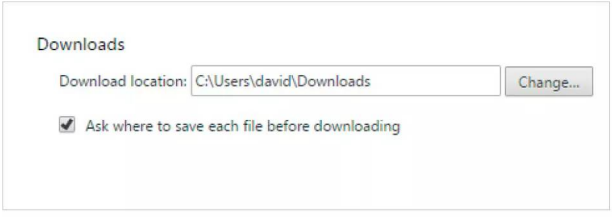
STEP 6 Click the Done button when you're finished with Content Settings, to return you to the Chrome Settings page. Within Privacy still, ensure the last option, Send a "Do Not Track" request, is ticked. This will stop any tracking elements from monitoring your browsing activities.



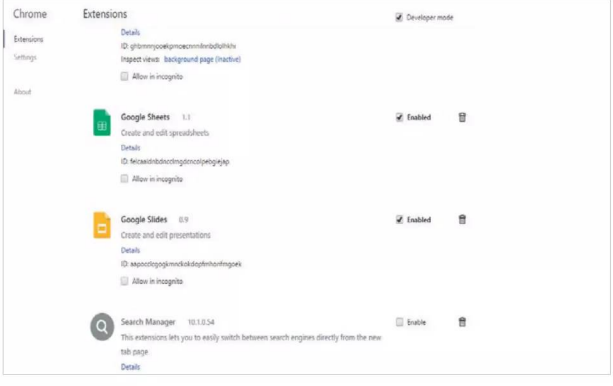
STEP 7 Just under the previous step's tick box, it's also recommended to untick the two Passwords and Forms boxes that offer to enable Autofill and Save your Passwords. Whilst it's a pain to constantly enter passwords, this will stop any hijack Chrome attacks from gaining your usernames and passwords.



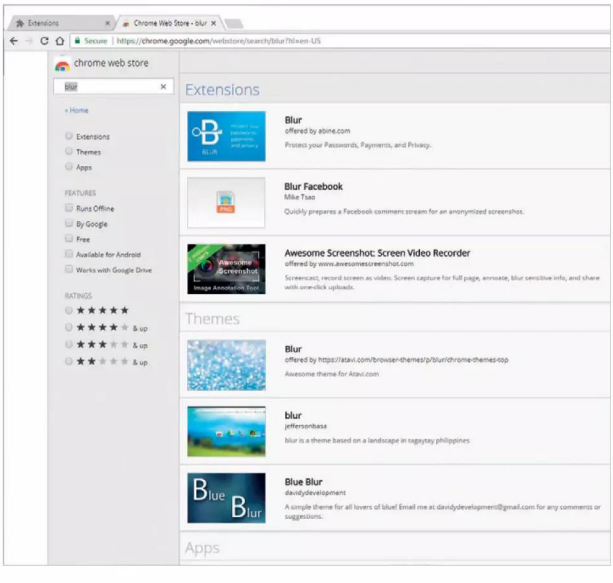
STEP 8 Under the Downloads section, it's an idea to tick the box Ask where to save each file before downloading. Again this can be a bit of a pain for the user; however it stops malicious background downloads from infecting your system, giving you more control and the ability to stop the process.



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



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



How to Secure Your Home Network

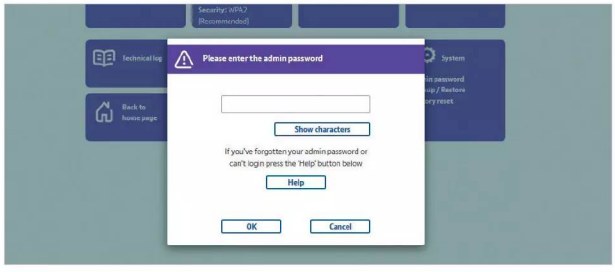
We've mentioned previously that an attack doesn't always come from the other side of the globe but can indeed be a little too close to home at times. Home network hacking is possible with the simplest of tools available on the Internet, often even just tapping into a cable.

Network Protection

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

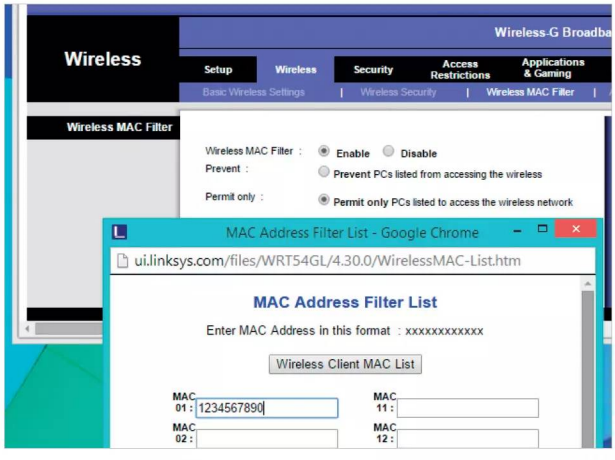
ROUTER PASSWORD

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



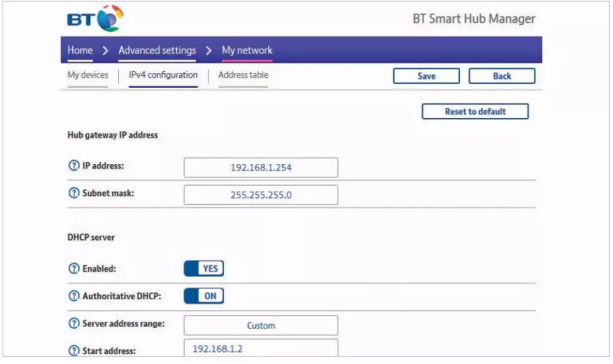
MAC ADDRESSING

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



DISABLE DHCP

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



POWER OFF

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

POWERLINE ENCRYPTION

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

ETHERNET CABLES

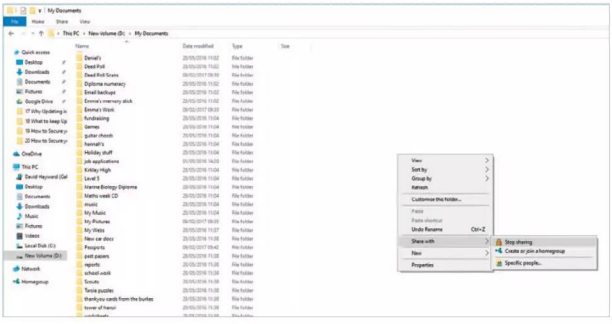
Cabling a home with Ethernet isn't a difficult project, this offers faster connection speeds than that of wireless; but if you're living in shared accomodation or a flat block, make sure that any unseen cable lengths can't be access by a neighbour. It's easy enough to splice into an Ethernet cable and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

NETWORK MAPPING

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

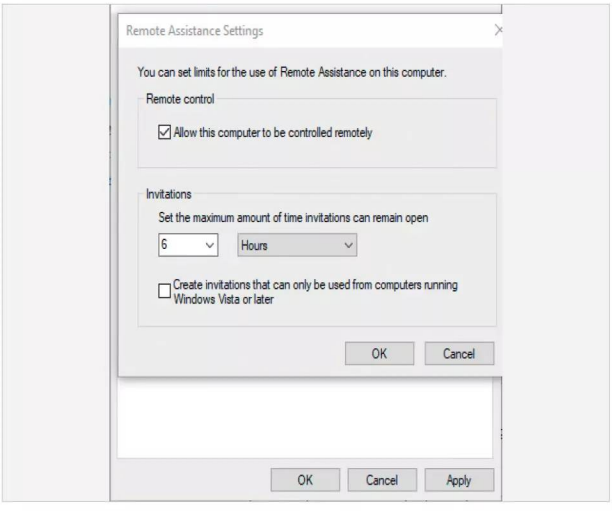
SHARE LESS

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



REMOTE ACCESS

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



VISIBLE PORTS

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

What are Wireless Security Standards?

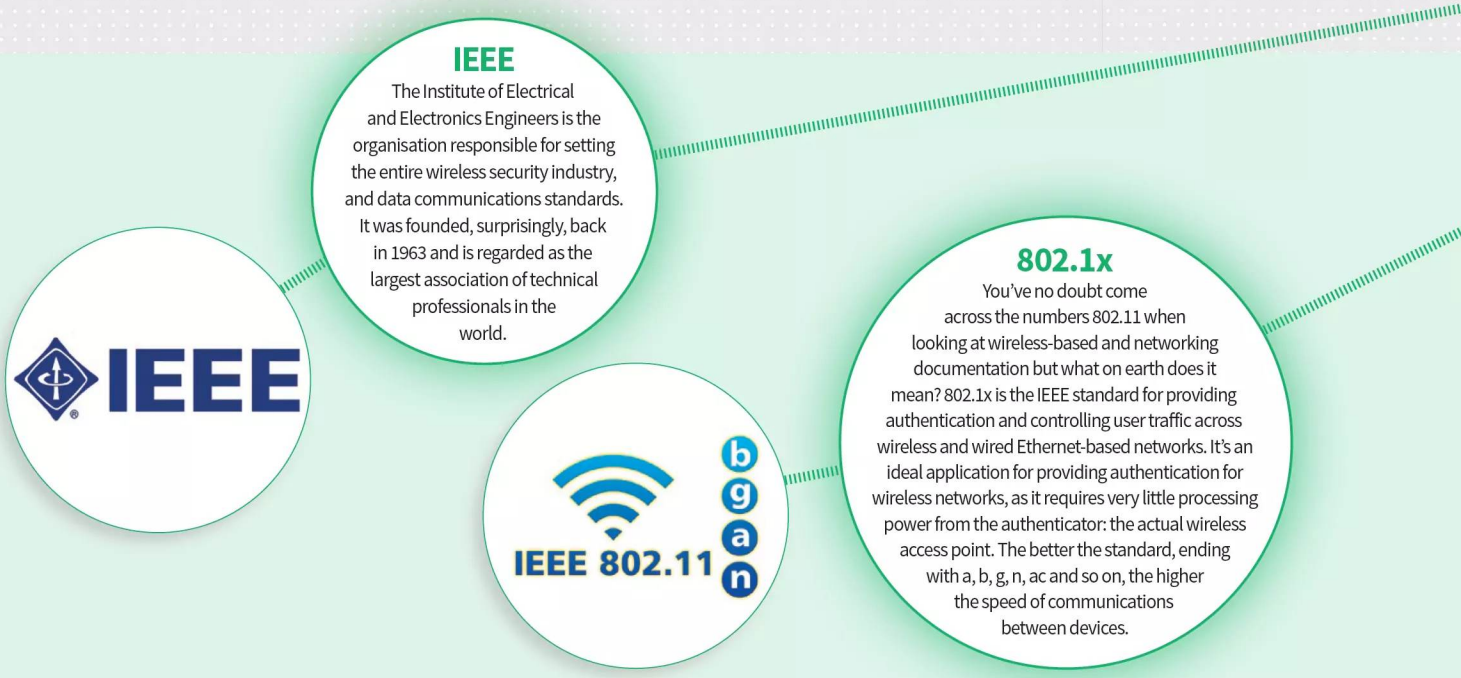
Wireless security has adhered to a number of standards since 1999, each improving over the last due to the ability for a then-modern computer to hack the security levels behind them. Tighter controls are needed as computers and the way they connect have become increasingly more complex.

WEP, WPA, WPA2, IEEE…

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

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

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



WPA2

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

WEP

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

Access Point

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

WPA

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

How to Secure Your Wireless Network

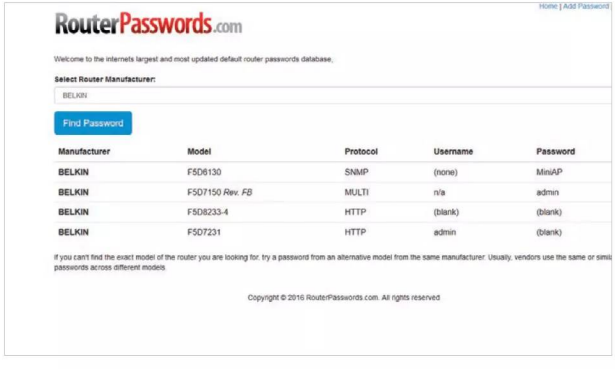
It may seem a little far-fetched but it's not unfeasible for a hacker to sit outside your house with a tablet or laptop and gain access to your home network via the router's Wi-Fi signal. Understandably it's quite rare but it's worth considering beefing up your protection.

Wi-Fi, Lock and Key

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

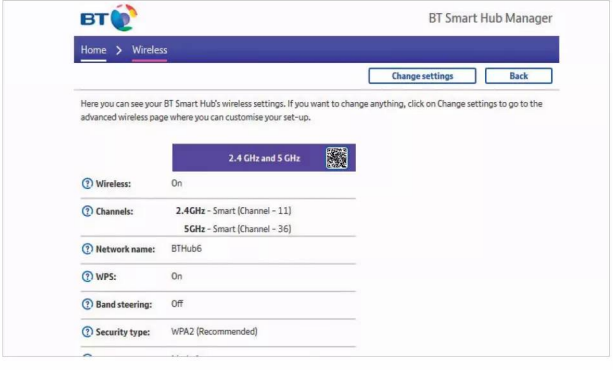
ADMIN PASSWORD

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



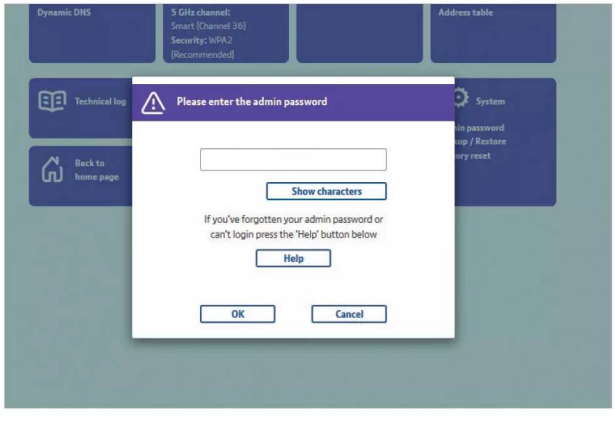
CHANGE SSID

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



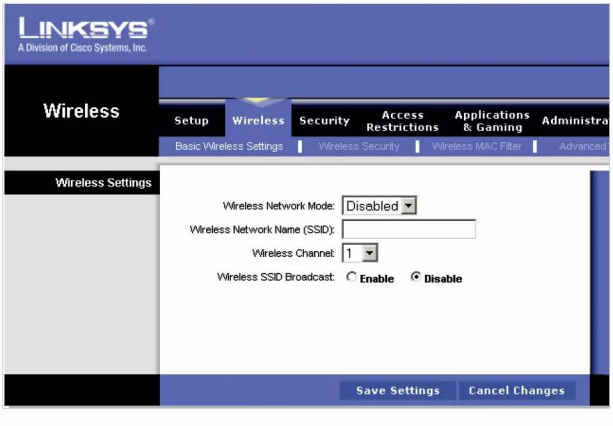
ISP PASSWORD

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



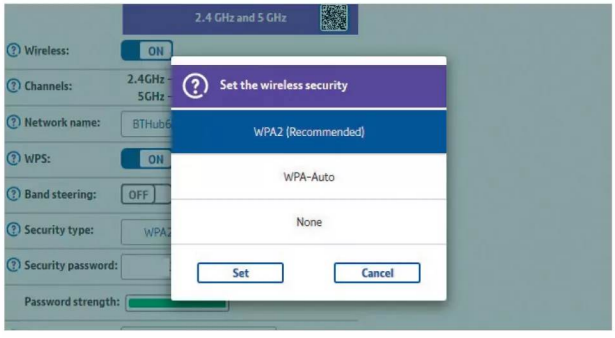
HIDE SSID

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



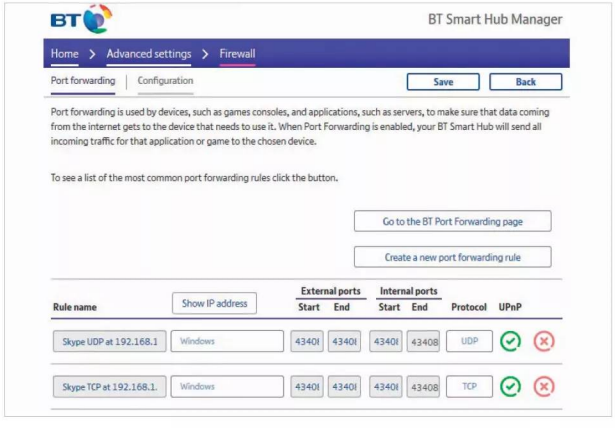
USE WPA2

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



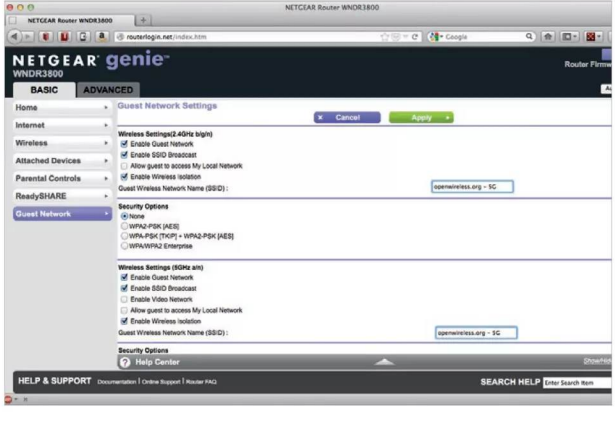
ROUTER FIREWALL

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



DISABLE GUEST

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

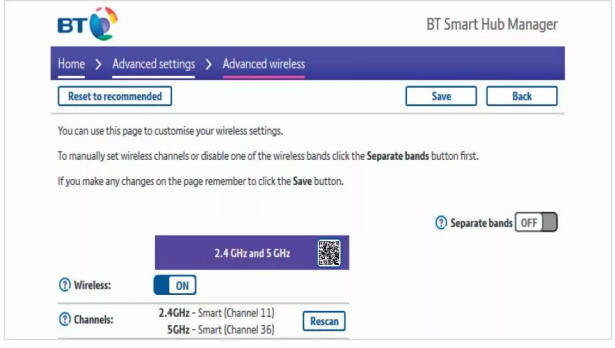


ROUTER RELOCATION

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

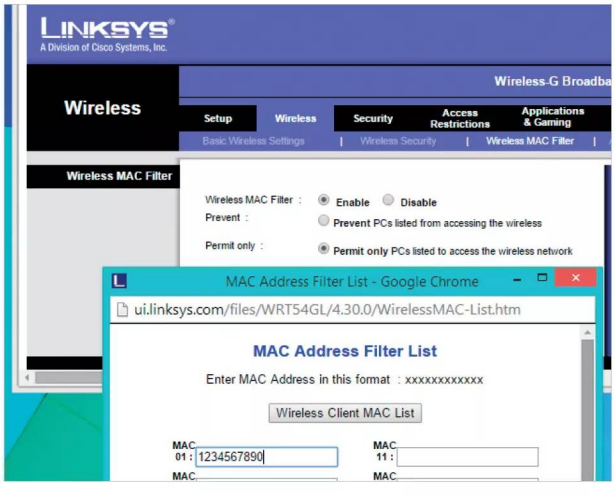
DISABLE WPS

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



MAC FILTERING

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



What is Encryption?

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

Kryptos Communications

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

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

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

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

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

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

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

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

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

> *Encryption is the act of protecting your data from prying eyes*

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

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

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

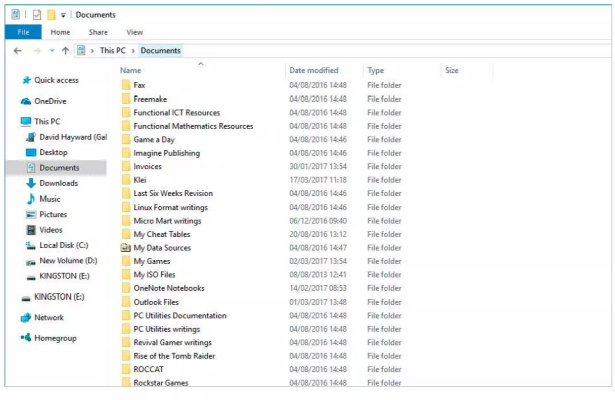
Encrypting Your Windows Laptop

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

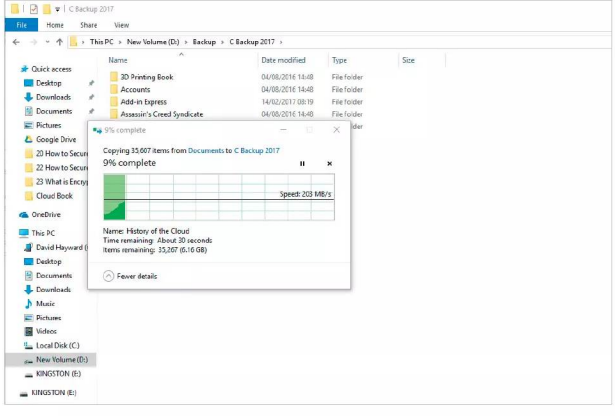
Windows, Under Lock and Key

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

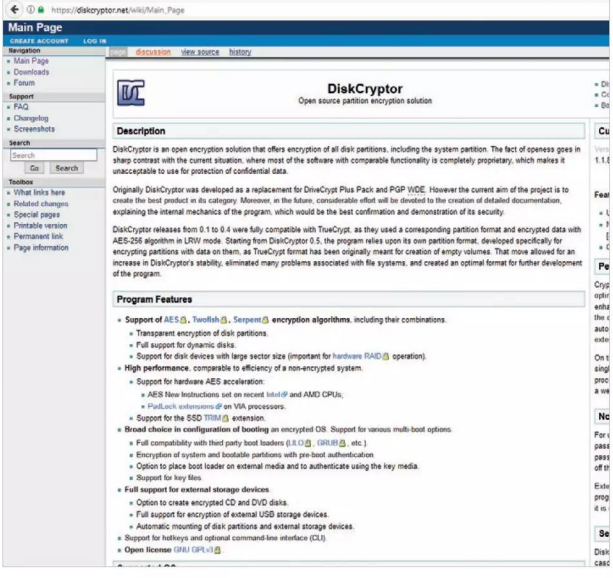
STEP 1 Encryption doesn't affect the core data, other than making it impossible to read without the decryption key but it's always worth making sure you have a backup of all your data prior to any system related changes. If you store your work or data in the Documents folder, then start by opening it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



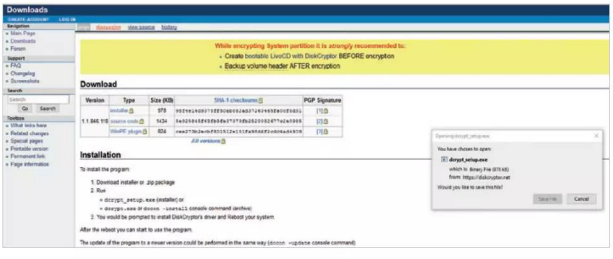
STEP 2 Press Ctrl+A to highlight all the files, then press Ctrl+C to copy them to the clipboard. Next, choose a suitable backup location such as an external or network drive and when ready, press Ctrl+V to paste the copied data into the new location. Then, should something go wrong, you have a recent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



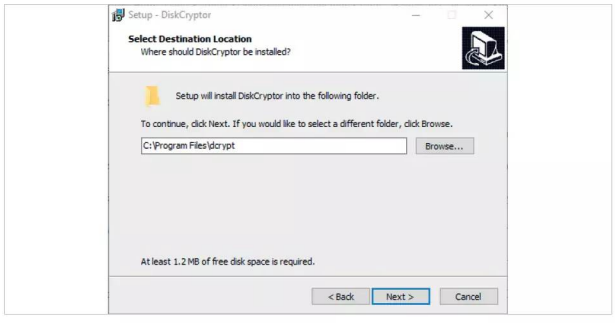
STEP 3 It's always best to ensure safe data before commencing with anything like this. It's also always worth doing (as we are) a test of the software first, on a disk that you don't mind messing up should you get the process wrong. Let's start by navigating to the DiskCryptor homepage, at www.diskcryptor.net/wiki/Main_Page.



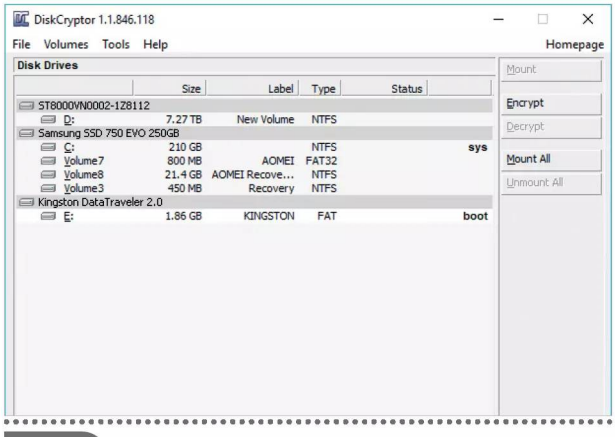
STEP 4 Using the menu to the top left, click on the Downloads link. Look for the latest version in the Download section and click the link for the Installer. This will open a confirmation box, click the Save File button to download the DiskCryptor executable file.



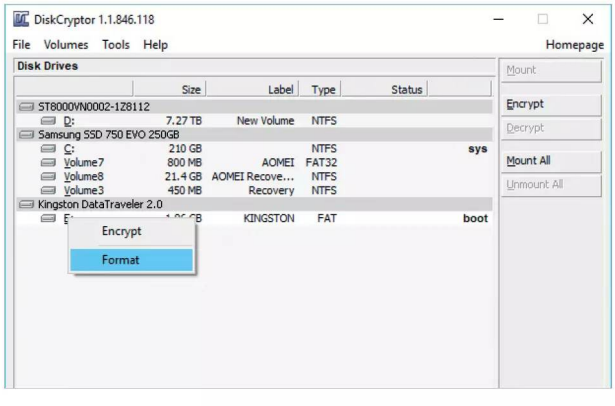
STEP 5 The dcrypt_setup.exe file should now be in your Downloads folder. Double-click it and select Yes to accept the Windows confirmation. With the DiskCryptor setup window open, click the Next button and accept the license agreement on the following page. For the remainder of the options choose the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



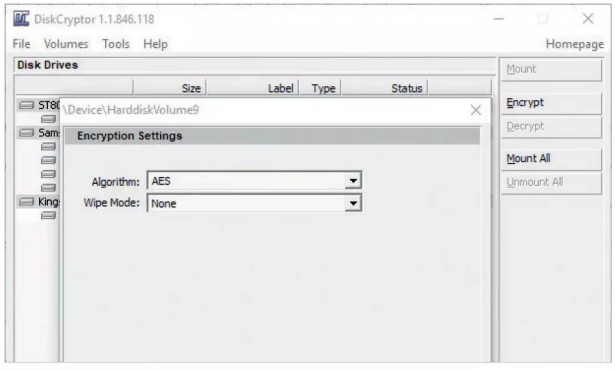
STEP 6 After a reboot, click the Windows Start button and locate the newly installed DiskCryptor program. You will need to click Yes to authorise its administrative access. With DiskCryptor open you can see the list of currently installed hard drives in your system. You can click each in turn and view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



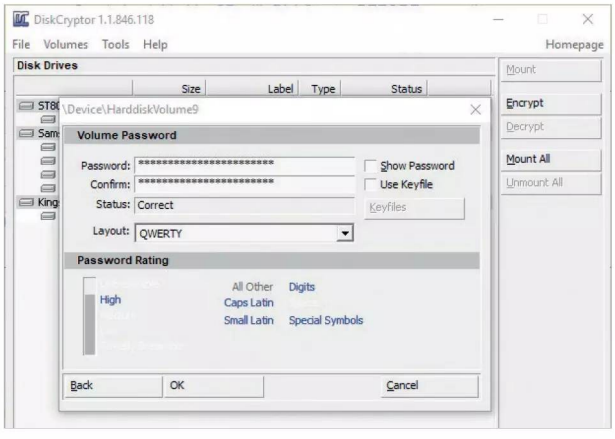
STEP 7 Start by selecting the disk you want to encrypt. In our example, as mentioned before, we're going to test this out on a USB stick. We recommend you do too, until you're comfortable with the process. With the correct drive selected, either click the Encrypt button to the right or right-click and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



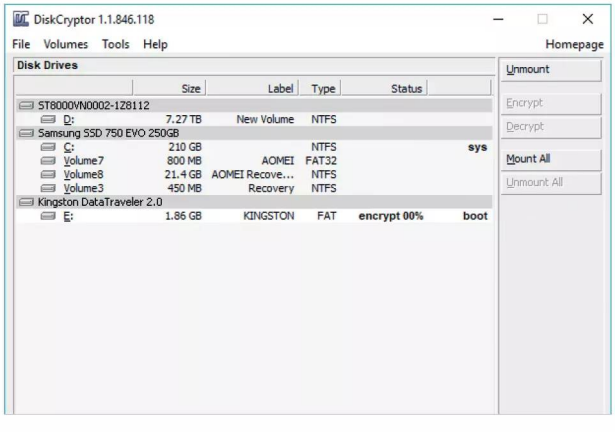
STEP 8 You're now offered a selection of available algorithms to choose from. Click the drop-down box to view them all but we recommend staying with the default AES algorithm for the time being. Leave the Wipe Mode box as None and when you're ready, click the Next button.



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



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



Top Ten Encryption Tools for Windows

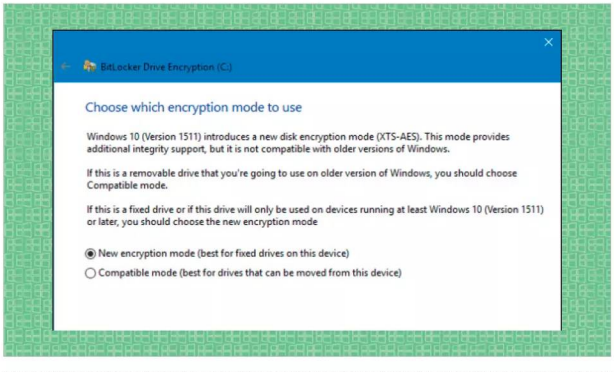
There's no shortage of programs that can encrypt files, folders and entire drives for Windows. Whilst some are very good indeed, others tend to fall by the wayside by not offering as good a solution.

Encryption Galore

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

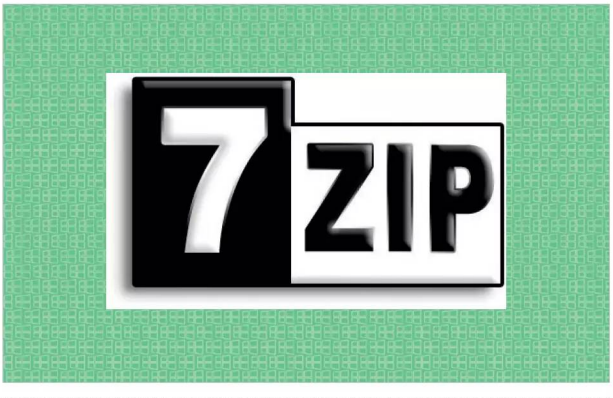
BITLOCKER

Available only for users of Windows Pro, Windows.1 Pro and Enterprise and Windows 7 Enterprise and Ultimate versions. If you're running the Home versions, you'll need to upgrade via the Microsoft site, or from the Windows Store. In short, BitLocker offers full disk encryption with 128-bit or 256-bit AES standards.



7-ZIP

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



VERACRYPT

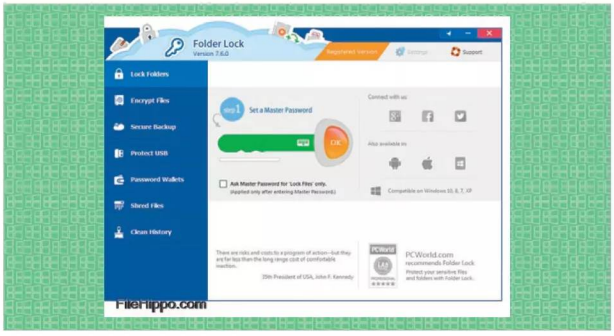
This is a free disk encryption program that's based on the popular TrueCrypt. It offers enhanced security, lots of levels of encryption and support for UEFI drives. It's available for Windows version 7 onwards as well as Mac OS X, Linux and even the Raspberry Pi.

AXCRYPT

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

FOLDER LOCK

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

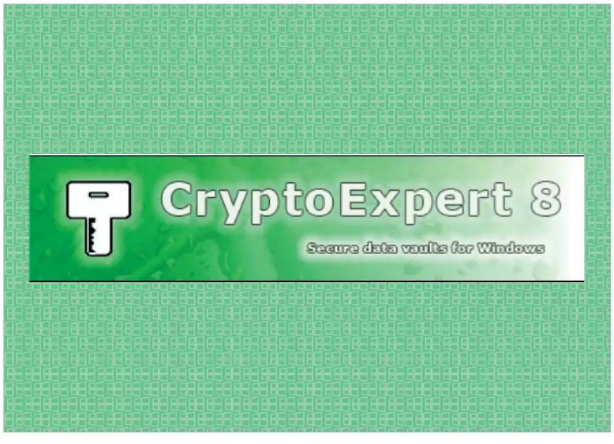


GPG4WIN

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

CRYPTOEXPERT 8

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



DEKART PRIVATE DISK

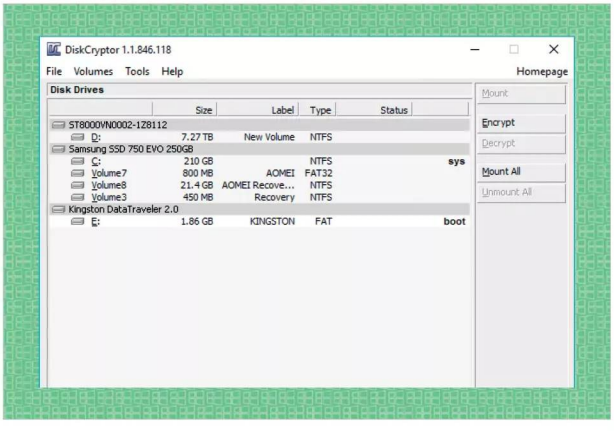
This is a simple and easy to use program that supports AES 256-bit encryption, compatibility with Windows Mobile, free unlimited support and updates; and it also includes its own firewall to help prevent hackers from gaining access to your system.

CERTAINSAFE

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

DISKCRYPTOR

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



What is a VPN?

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

Virtual Private Network

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

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

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

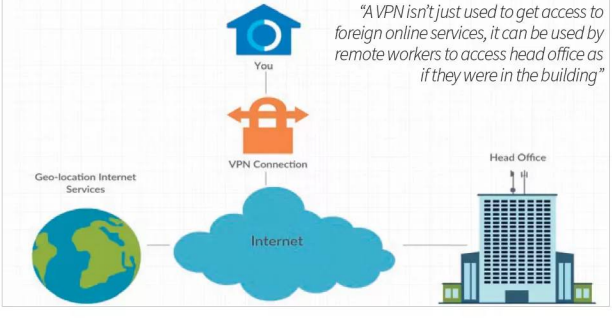
However, for most users having a VPN means they're able to gain access to TV channels in the U.S., Canada, Europe and other parts of the world. It's not always about being able to moderately 'cheat the system' by forcing the Internet to think you're somewhere else other than where you actually are though.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

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

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

There are plenty of VPN providers to choose from and we'll look at ten of the most popular in a while. Some offer a free connection service that's handy for quick browsing but isn't very fast. To gain access to faster servers, with better security and protection features you need to pay a monthly or annual subscription fee. Thankfully it's not a lot, for the most part: you'll be expected to pay in the region of £5 to £15 per month. This grants you better coverage and the ability to use up to five or more different devices, including tablets and phones.

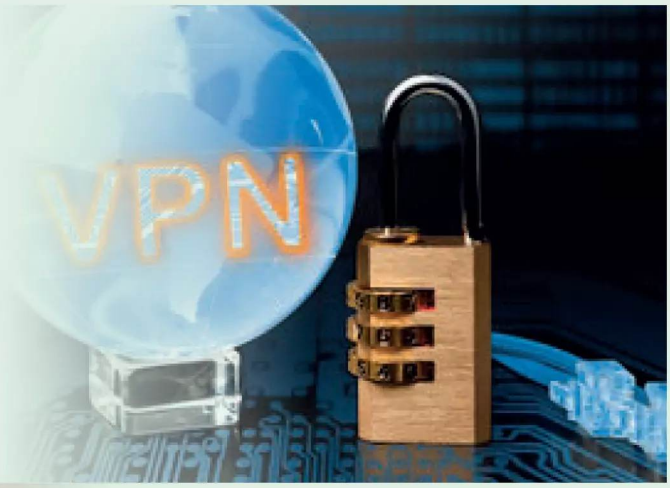
Over the coming pages we dig a little deeper into VPNs, as you can imagine, using one will significantly improve your protection when online. In terms of Windows security, the use of a VPN is quickly becoming vital, so by the end of this chapter you'll be knowledgeable and helpfully utilising one to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

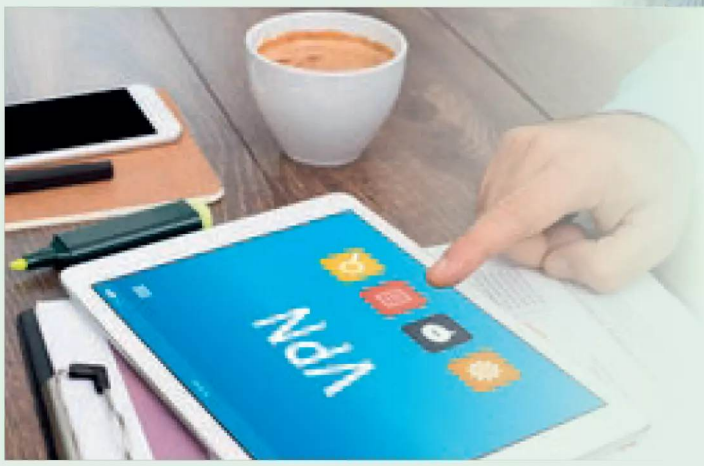


"A VPN isn't just used to get access to foreign online services, it can be used by remote workers to access head office as if they were in the building"

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

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





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

How Can a VPN Improve Windows Security?

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

Security Beyond Anonymity

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

BROWSING ACTIVITY

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

ANTIMALWARE

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

THREAT PROTECTION

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

HIGHEST ENCRYPTION

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

WI-FI PROTECTION

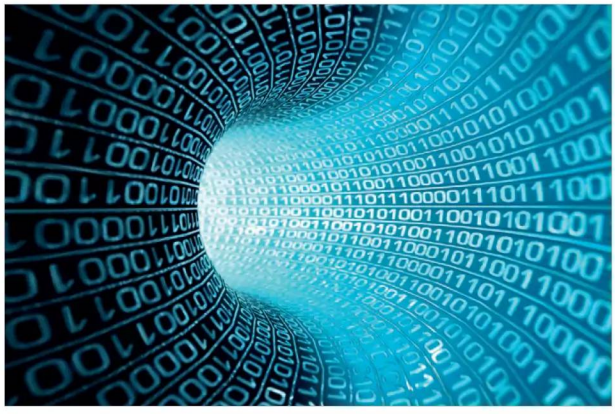
Public and free Wi-Fi hotspots are notorious when it comes to mobile security. Anyone with a little knowledge and some free tools via the Internet can intercept public Wi-Fi network and hijack your connection, revealing all your data. A VPN will encrypt the data and protect you.

AD BLOCKING

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

SECURE TUNNEL

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

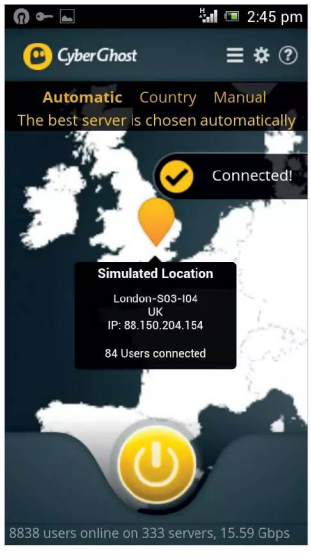


USE HTTPS

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

MULTI-PLATFORM

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



ZERO LOGS

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

Top Ten VPNs

When it comes to ensuring your data doesn't fall into the wrong hands, there are plenty of VPN options out there. The service runs on your computer, smartphone or router and encrypts all your internet traffic and forwards it through a secure server.

VPN Services

Listed below are a number of popular VPN services. The services on offer are subscription-based and they all ensure that your privacy is maintained. For a relatively small monthly outlay, you can be anonymous and even unlock access to sites previously blocked by your ISP.

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

NORDVPN NordVPN offers two levels of encryption, access to fast servers, no logging, a kill switch in case the VPN connection drops and you're still surfing and support for multiple devices and operating systems. It's well priced and is highly regarded among the press and media.

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

PUREVPN With support for multiple devices, 256-bit AES encryption and access to 180 locations worldwide with 750 plus servers, PureVPN is a great choice for the home user. The cost varies depending on the package but Just as with all these VPNs, it's worth checking for the latest pricing.

VPN UNLIMITED

VPN Unlimited offers a full firewall service with anti-malware, ad blocking and anti-tracking. There's 256-bit AES encryption, over a thousand servers in 70-plus locations, support for up to five devices, fast servers and app support for iOS, Android and Widows Phone. Pricing varies so it's wise to check.

PRIVATE INTERNET ACCESS

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

IPVANISH

IPVanish is another highly regarded and awarded VPN service. Depending on the package, you get access to fast servers, unlimited bandwidth, no logging, 256-bit AES encryption and support for up to five different devices.

VYPRVPN

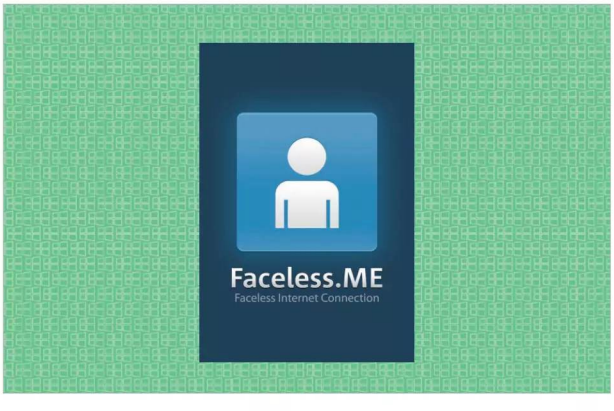
VyprVPN is an exceptionally good service that offer access to fast servers, multiple device support, unlimited bandwidth and connection, 256-bit AES encryption and access to over seventy global locations and hundreds of servers.

TUNNELBEAR VPN

TunnelBear VPN offers an initial 500MB per month free service, increasing in price for unlimited bandwidth. For this you get access to fast servers across twenty plus countries, 256-bit AES encryption and support for Windows, iOS, Android, macOS and browser add-ons.

FACELESS.ME

Faceless Me is an interestingly named VPN service. Amongst its features expect to see elevated levels of encryption, unrestricted access, an easy to use interface and unlimited traffic. You get 2GB per month for free but you can pay a monthly subscription to have unlimited access and traffic.



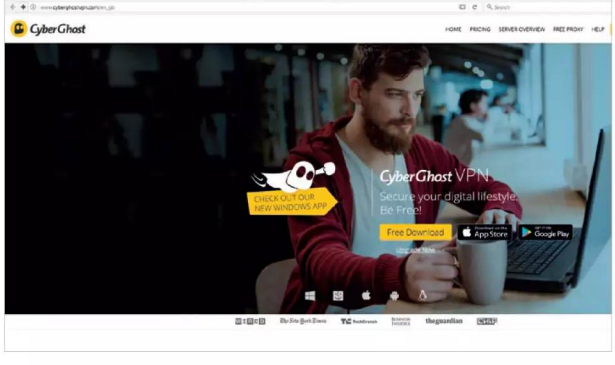
Using a VPN for Added Security and Privacy

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

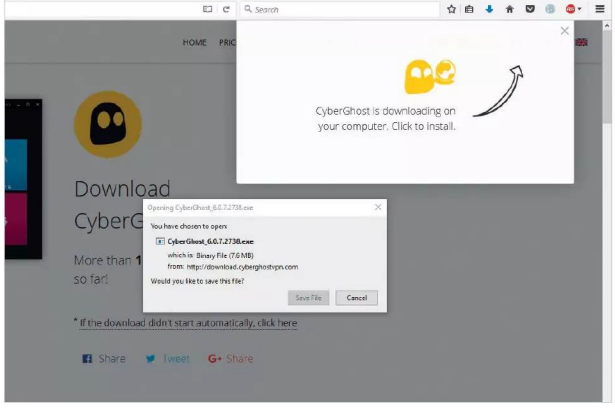
CyberGhost

We're going to use CyberGhost as the example VPN for this tutorial. You'll need to purchase one of the available packages to begin with. You can choose from a rolling monthly subscription of £9.99/mo or up to a three year plan billed £68 every three years.

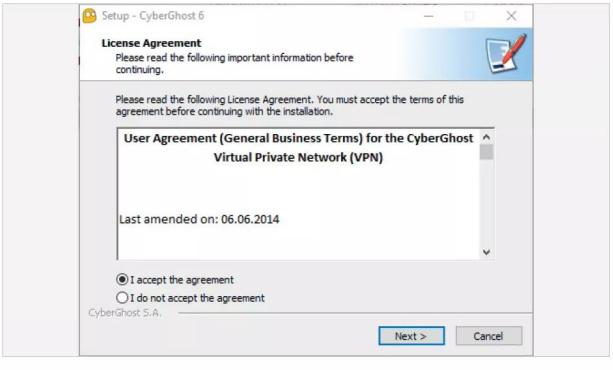
STEP 1 We won't use the free option in this instance, as the paid for services offer a better set of features with which to display the VPN in action. Start by navigating to www.cyberghostvpn.com and clicking on the Pricing link in the upper portion of the main CyberGhost site for your regional and latest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



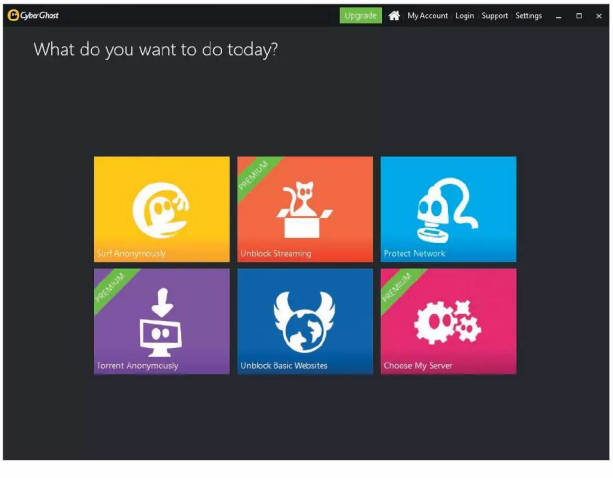
STEP 2 Assuming you've purchased one of the options, click the yellow Free Download button located in the top right of the main page. This will, after a few seconds, automatically initialise the download of the latest CyberGhost client software. Click Save File to download it to your Downloads folder.



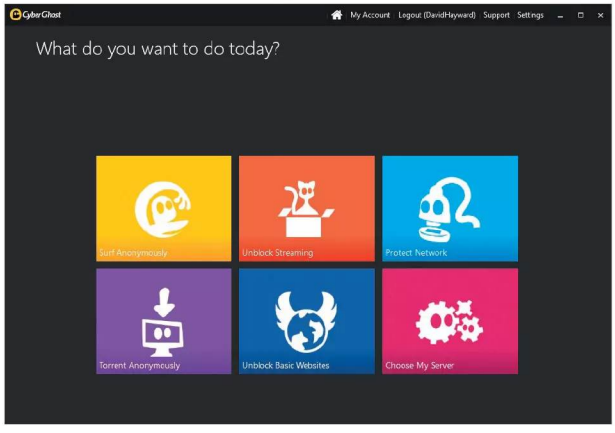
STEP 3 Go to the Downloads folder and double click the CyberGhost executable followed by a click on Yes for the Windows authentication process. Accept the agreement and follow the on-screen instructions to set up CyberGhost on your PC; the default options are fine to use, unless you specifically require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



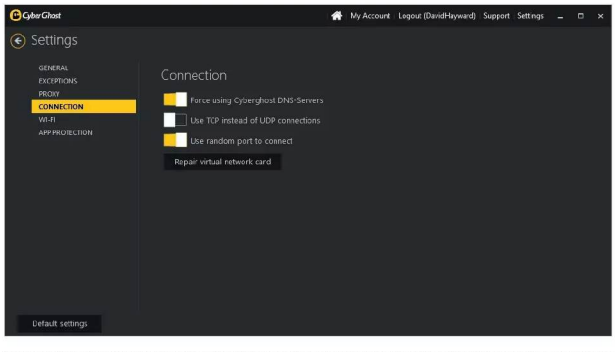
STEP 4 Once the installation is complete you're presented with the main CyberGhost client window. However, before you make a connection, click on the Login link located at the top of the client window.



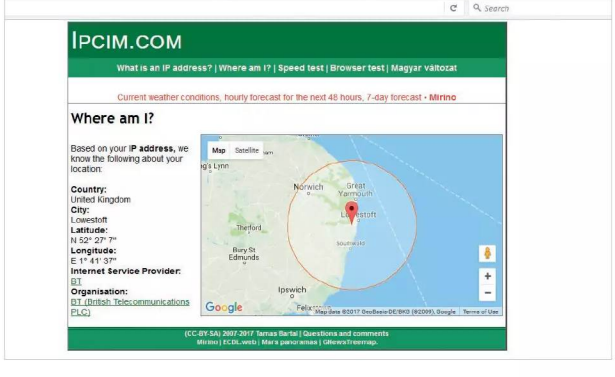
STEP 5 Enter your CyberGhost login and password that you set up when you purchased the package and click the OK button. Once the login is confirmed you're taken back to the main client window where the available options for the account package you purchased will be displayed.



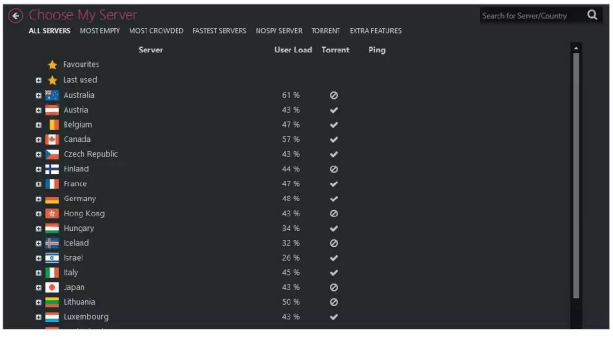
STEP 6 Before you use the service, it's best to check a couple of things. First click on the Settings link along the top of the client window. In here you can see multiple options for the control, connection and how CyberGhost will work with your PC. Generally speaking, the defaults are fine unless you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



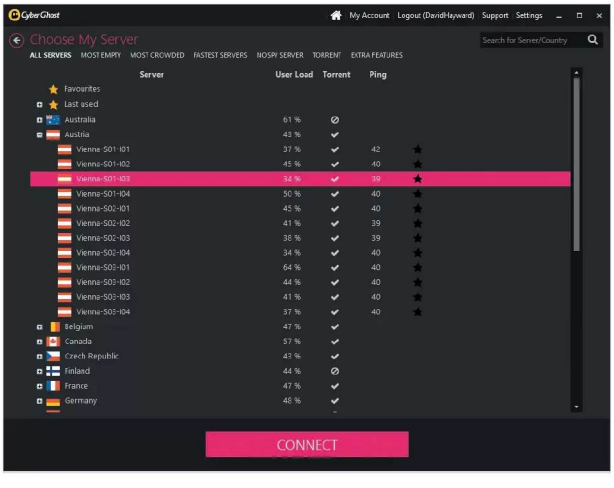
STEP 7 One more thing before connecting to the CyberGhost VPN: open a browser and enter www.ipcim.com/en/?p=where. This will display detailed information based on your IP address, such as the ISP you're using, the country, city, even latitude and longitude, complete with a map and possible radius you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



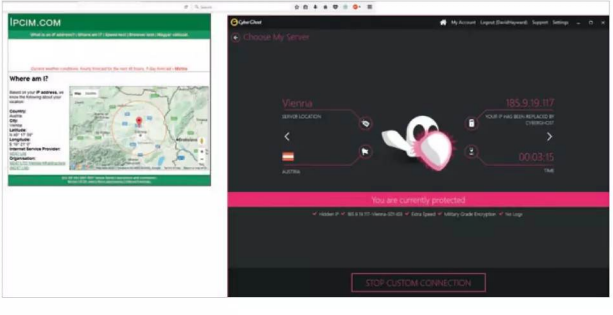
STEP 8 Click back to the CyberGhost client and return to the main window. Click the Home icon along the top of the client window and then the Choose My Server button in the bottom right. This allows you to choose your own server from the available countries that CyberGhost works with.



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



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



Read More

Now you've got the basics down, you can improve and learn more essential skills in our next level guide...

Now Available on

Readly

www.pclpublications.com

Home Networking For Beginners

6 I ISBN: 978-1-912847-15-0

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: james@papercutltd.co.uk