Essential Technology Guide

Home and Small Business
2017 / 18

Computer AMBULANCE
Serving Residential & Small Business

A year in review.

2016 was another year when technology moved at a blistering pace. Cloud computing has gone from being an abstract geeky term to becoming part of our everyday vernacular. Front-end computing devices, such as tablets and smartphones, have become more powerful, lighter and thinner, and fixed-line and mobile internet speeds are now faster. Technology continues to pervade nearly every aspect of our lives, but perhaps the most significant changes did not happen with front-end devices, but rather with behind-the-scenes technology that most users will never even get to see. Computing is set to be revolutionised by its gradual transition from number crunching to artificial intelligence (AI).

Back at the front-end of things, 2016 was the first year in which we noticed frissons of discontent among some Irish Apple users, due in part to issues with faulty GPUs, flaky iCloud services, buggy iPhones and many other niggles. Even long-time professional users of Apple, such as graphic designers and photographers, are now grumbling about the company – an ominous portent when it was these same users who helped to propel this once niche computer brand into the mainstream. Moreover, Apple has not released a truly innovative product for the longest time frame (in recent history at least), and instead seems to be content making only incremental changes to its existing product lines. For example, they have removed the standard headphone jack on their latest iPhones and replaced it with a proprietary wireless connection. Innovation for innovation's sake? Maybe. But meaningful innovation at Apple seems to have plateaued and the honeymoon period between the brand and some of its user base is well and truly over.

In Microsoft land, 2016 will be remembered as the year of the involuntary operating system upgrade. Some users who had left their Windows 7 computer on overnight, woke up the next morning to discover that Windows 10 had installed itself by the following morning. This invisible hand of Microsoft foisting upgrades on its users annoyed many. Not least one Californian travel agent who was so annoyed with a forced Windows 10 upgrade that she sued them at her local small claims court and was awarded $10,000 for the business she had lost during the interruption to her business. These issues aside, users are slowly getting used to Windows 10 in the same way that drivers get used to the controls and switches in a new car. Moreover, Microsoft seems to be finding its groove again with new computing devices, such as the Surface Pro tablet. While it might not beat the iPad and its extensive ecosystem of apps, it has wowed many for being a sleek, fast and no-nonsense business device.

And it's not just Microsoft and Apple who are innovating. 2016 will go down in the history books as the first year ever where a mass-produced pure play voice-controlled computing device became commercially successful. The Amazon Echo Dot is a small hockey puck sized device that allows you to control the temperature in your house, order a taxi, play

an audio track or even order a pizza, just by speaking. While devices like the Echo Dot possibly offer a foretaste of the future of human-to-computer interaction, it is also a great example of the power of AI. It is connected via the internet to Amazon's cloud-based voice service Alexa, which can hear and understand human questions like "what is the weather forecast for Dublin tomorrow?" or "I need a taxi".

While devices like the Amazon Dot Echo can make our lives easier, we are continually reminded about the fragility of technology. Hardly a week passes without hearing another story or headline about computer hacking. Not so long ago, hacking was something that only happened in Hollywood movies, now it has become almost a daily occurrence. In February last, the biggest cyber-heist in history took place when $81 million was stolen from the Central Bank of Bangladesh. In May, it was discovered that 117 million LinkedIn accounts were hacked and subsequently sold on the so-called dark web. October saw a massive DDoS (distributed denial of service) attack on Twitter, Spotify and Reddit. Hackers, using already hacked webcams and digital recorders, bombarded these sites with junk traffic and temporarily brought them down. The first architects of the internet designed their "inter-network" so that it could sustain a nuclear attack, but they probably never envisaged that such a mundane piece of technology, such as a webcam, could take it down. The prospect of power grids, transport and banking systems being brought down in a similar manner is a frightening prospect. Aside from DDoS attacks on popular websites, the past year showed the most pernicious effect of hackers as thousands of Irish computer users had their Windows and Mac systems attacked by so-called ransomware. This extremely damaging malware, propagated mainly via "phishing" emails, did untold damage to users of PCs and storage devices by maliciously encrypting important data, such as accounts files, Word documents, PDFs, photos and music.

While cyber-attacks remind us about the fragility of the internet, we are also reminded of its omnipotent power. It has disrupted nearly every industry imaginable. In the past year, Airbnb rented out more rooms than all the big global hotel chains combined together. Television and film companies have been disrupted by Netflix. The music industry was first interrupted by peer-to-peer file sharing services, then iTunes and now streaming services, such as Spotify. While Taxi services in areas across the globe have been disrupted by Uber-type services, and this is just the tip of the iceberg. When AI (or machine learning) starts to converge with existing technologies, it will have profound changes on the way that we live and work. Some twenty years ago, when Bill Gates predicted that the internet would "change everything", many listened to this proclamation with a pinch of salt. And here we are, almost twenty years later and his prediction has largely been borne out.

AI will have a similar trajectory. We are already seeing tiny glimpses of this technology, with e-commerce platforms, such as Amazon, already accurately predicting our product preferences. Media companies, like Associated Press and Bloomberg, are now using AI to auto-generate headlines for their TV and internet channels. The state of British Columbia has introduced AI into its small claims court to process housing disputes.

The Netherlands have introduced their AI-powered "Rechtwijzer" system to propose solutions for couples who are separating or divorcing. Cars can already self-park and self-driving vehicles are now imminent. In the world of medicine, software such as Enlitic can assist doctors to analyse x-rays and CT scans faster and more accurately. Surveillance technology, such as Graydient-V, can perform real-time anomalous behaviour scanning from security camera footage. This improves security monitoring whilst also reducing the need for security personnel. Even in sectors such as agriculture, AI is set to transform the way that farmers work. Innovations like the LettuceBot can scan 5000 plants a minute, using algorithms and machine vision to differentiate between good crops and weeds. This means that rather than spraying a whole field, herbicides can be applied only where they are needed with laser-like precision, saving the farmer cost and resulting in more organic and healthier produce. Or consider the Irish-invented MooCall system, which uses a sensor attached to a cow's tail. This is powered by smart algorithms that can forewarn a farmer via SMS or web portal when his cow is about to calve.

Technology will transform the workplace as we know it. Pessimistic outlooks from think tanks, such as the World Economic Forum, claim that technology will create around 2 million jobs by 2020, but it will also displace around 7 million. However, history has shown that while technology will inevitably displace some occupations, it also has a happy knack of creating spin-offs and entire new industries. In the early 1900s, the nascent car industry led to a massive decline in work for carriage makers and other horse-related industries, but spawned new industry sectors, such as car insurance, motels, out-of-town recreation facilities and shopping complexes. Thirty years ago, who could have imagined there would be occupations, such as web designers or e-commerce architects? And even with AI, technology problems still exist and robots have not replaced the need for IT support (not yet at least...).

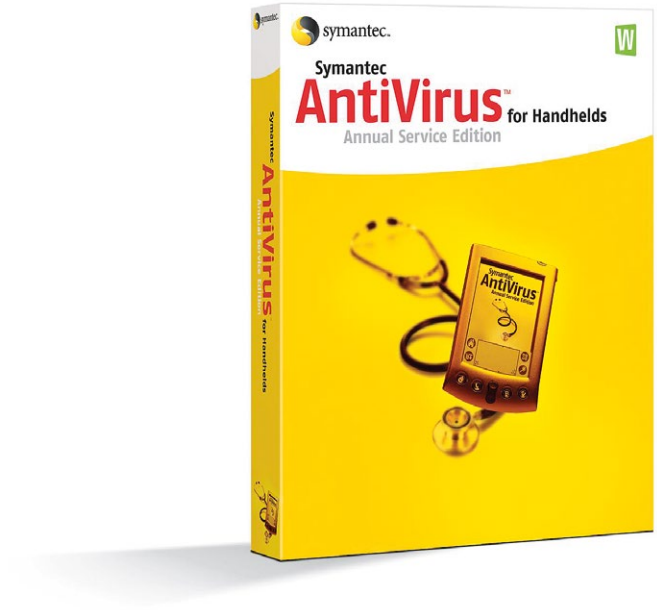
I would like to take this opportunity to thank you for your continued custom with us. During 2016, Computer Ambulance engaged in minimal paid advertising. Instead, we had the best sales team any business could ever wish for – you! And for that, I am very grateful. We look forward to offering you a first-class technical support experience again during 2017.

Best Regards,

Rob Scanlon
Founder
Computer Ambulance

Why isn't anti-virus as effective as it used to be?

Many users are still shocked to learn that anti-virus software is not nearly as effective in protecting your computer as it used to be. There are many reasons why it has lost its clout.



This is partly due to the growing ineffectiveness of signature-based (or definitions-based) detection that is still widely used by the security software industry. This is good at detecting known threats that have been floating around in cyberspace for a while, but when threats are unknown or derived from existing malicious code and tweaked to evade detection, signature-based detection can be a porous filter from the millions of threats in existence. IT security software companies have responded to these changes by using more heuristic-based (behaviour-based) scanning. But just as heuristic scanning engines have become smarter, more viruses now use metamorphic code, which means the virus can edit and rewrite its own code and so change its behaviour on the fly. Even more undetectable are polymorphic viruses. These encrypt their own payload to help them fly under the radar of security defences and only decrypt themselves just before the payload is released.

Another reason why anti-virus products are less effective is due to the huge increase in "zero-day" vulnerabilities. These are exploits designed to attack vulnerabilities in computer applications, operating system or firmware code that security researchers have not yet discovered. Free "exploit-kits" can be easily acquired on the dark web with more sophisticated versions. No matter how good security researchers are, there are always going to be "gaps in the fence" that malicious hackers can use to subvert even the strongest of defences.

The proliferation of "blackware" laboratories have also contributed to the lack of anti-virus effectiveness. For years, professional IT security companies have been using honeypots to capture the latest type of malware. Once captured they would decompile it, analyse it and then use what they had learnt to build better IT security products (such as anti-virus, anti-malware software etc). This approach worked well for years. But virus and malware authors are now using the exact same reverse-engineering techniques of the anti-virus software companies. They have developed their own "anti-security" laboratories to analyse anti-virus products and patches that are issued by Microsoft and Apple. They test their own exploits against well-known IT security products. So the tables have well and truly been turned, as these blackware laboratories are now trouncing the R&D capabilities of established security software players, like McAfee and Symantec.

So if anti-virus isn't as effective as it used to be, is there anything I can use to make my computer safer and prevent ransomeware from infecting my system?

Most users have now heard the horror stories of friends, colleagues or family members who have had their computers infected with file destroying ransomware, such as Cryptolocker and its variants.

There are a couple of measures that you can take to help mitigate against such attacks, including:

Always make sure that your **operating system and application software is up-to-date and patched**. Running out-of-date software on your PC or Mac is like having a car with bald tyres, cracked windscreens, no mirrors and bad brakes.

Watch out for the three amigos of computer insecurity, **Adobe Reader**, **Flash** and **Java**. Unfortunately, these continue to be exploited by virus authors and hackers. They should always be kept up-to-date.

Don't open any suspicious attachments. This includes the treacherous .ZIP format, which is often a conduit for some of the nastiest payloads around. Others to watch out for include .RAR, .VB, .BAT and .DOCM files. A file attachment that catches many a user off-guard is the .JPEG or .JPG format. These can be used to hide malicious code that is only executed when the image is clicked on. Now most readers reading this will say, "I never open any suspicious attachments" or "most of those email scams are obvious". But that is the rock they will perish on. Most of these scams seem obvious in hindsight, but when a business person or office worker, who is suffering from information overload, receives several email attachments a day, the line between "safe-to-open" and "unsafe" becomes a little more blurred. Sometimes, it only takes two events to coincide and a previously "unsafe" email with attachment can get opened. For example, if a person is actually expecting a VAT refund and an email does arrive from the "Revenue Commissioners", there is a much greater probability of the scam being successful.

It is a good idea to use applications like **Hitman Pro Alert** to complement your anti-virus solution, as it detects trojans, rootkits, adware and other malware that your anti-virus program might have missed.

Also, make sure that your operating system is set to display the full file names. Many virus authors like to hide their executable (.exe) files with seemingly harmless ones like "picture_of_you_at_ party.jpg.exe". The ".exe" extension can be obfuscated to make it look like it's a harmless .JPEG file. To make sure the full file name always appears within Windows, go to Control Panel > File Explorer Options > View tab > uncheck "Hide extensions of known file types".

You should also make sure that all macros in Microsoft Office are disabled, as Macro viruses, which used to be extremely prevalent in the early 2000s, have now made a resurgence.

It is important to backup all your important data. Even if you're meticulous with your IT security there is always the risk of something slipping through the net. We suggest that you follow a 3-2-1 backup strategy. This means having three copies of your data, two of which are on different devices and one of which is off-site.

How safe is shopping and banking online?

Many computer users assume that if they see an "s" beside HTTP, along with a padlock icon in their browser's address bar, they are protected. Unfortunately, this tells only half the story. A HTTPS connection only means that the actual connection from your browser to a remote server is "safe". It tells you nothing about how safely your login details or credit card details are stored. For example, a website could be serving up malicious Javascript to you but your browser will still deem it be a "safe" connection.

Moreover, hackers can hijack some "secure" SSL connections. To help protect you against this type of attack the Electronic Frontier Foundation has produced a browser extension for Firefox and Chrome called HTTPS Everywhere, which forces your browser to use the encrypted version of a website whenever possible.

Now you might be thinking that surely a company like Google can come up with a more secure solution? Well, I'm sure they could but what most people don't know is that Google has a vested interest in maintaining the HTTPS protocol for as long as possible, as it makes it extremely difficult for any of their potential competitors to easily index websites.

How do I pick a secure password?

In 2004, Bill Gates predicted the demise of passwords, but more than a decade later they are still with us. When registering on a new website and setting a password, you've probably had your first or second attempt rejected because they did not meet the website's security requirements. This can be annoying for some, but it does at least signify that the website owners care about security. When picking a secure password, you have a strike a balance between security and usability. A password which you can never remember because of its complexity is not much good. Some users believe that leeting their passwords, e.g. m@nun1ted makes it more secure. It doesn't. Any hacker worth his salt with be using what are known as "rainbow tables", which are extensive databases of commonly used normal and leeted passwords.

So how do you pick a password that is both secure and memorable? This is where the Correct Horse Battery Staple method comes in. You simply pick four random words and join them together to form a password. For example, if you pick the words "correct", "horse", "battery" and "staple" to create the password "correcthorsebatterystaple", you actually have a very secure password that presents hackers with 1.1^24 permutations to crack it. Simple, secure and easy to remember.

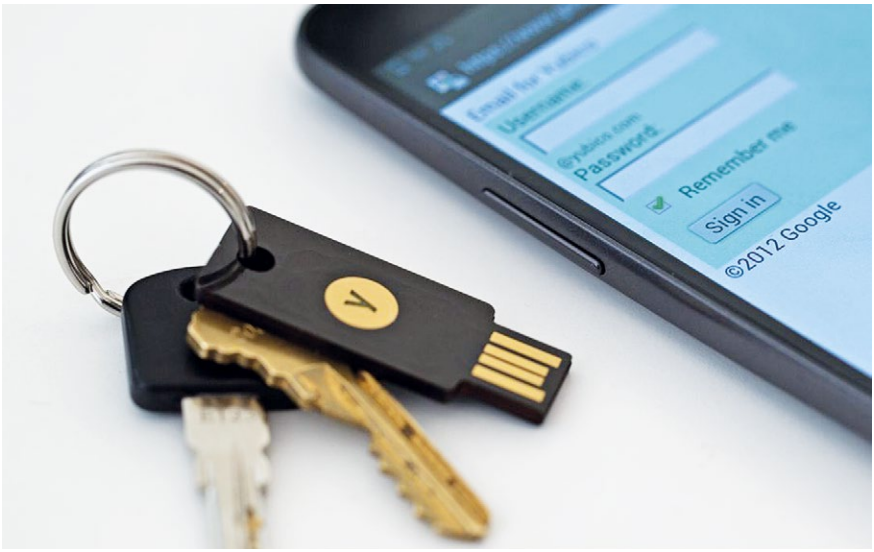
Passwords generated using the "Correct Horse Battery Staple" method:

```
NerdMistyType8          DiningMynahsElse4       OrlonsDudsFrat2
PalateDimlyRepute3      FriersMohoWhere7        ArgotCattleMourns6
SniffsDozeBayed9        ArnoJoveSulla0          DanaRubbleReins9
CaliphJiveKidder7       OrwellStayNiche2        RavedRosieSticks3
NashListerFrenzy2       CacaosSousaCobs1        PrayerClaimsRugs4
MetedDiesCashew4        MistedRaquelOsage9      IambsAryansSpiels9
PromptShapeDarn5        JivaroMambosFugues2     TootsIjsselMerger9
HafizAdvertSpoof2       ExcelBlazerWrack4       LouiseZensDiodes0
AdamSpainScents7        MusketDucksMaya5        DatumFratEscort3
YankeeSwoonsFuzhou9     TongaScarePapaya7       CartelUnbindArmors5
StillPaddleKlein1       BlackTenderMurphy2
```

Going beyond passwords to secure your Gmail account

Okay, so you've picked a really secure password for your email, which is easy to remember but complex enough for hackers to easily crack. Does this make you safe now? Unfortunately, not. There is an old adage in the IT industry that says "hackers can hack anything". This is largely true, given they have enough time and resources to do so. Your job as an end-user is to make the prospect of hacking you as difficult as possible, so that they will just move on to easier targets.

So if you want to make your email account really secure, you could employ a measure known as 2-step verification. Previously, with Gmail this involved inputting a code that Google would send you via text message. Thankfully, Google has now streamlined this rather clumsy process and so you can now verify your account with just the click of a screen.



There are some IT security experts who claim that even using a secure password and two-step verification is still not sufficient because if your phone was stolen (or your SIM card has been cloned) the hacker would have access to your verification code. To counteract this (and if you're really security conscious) you could configure your Gmail account to use two-factor verification with a device like the Yubikey, which is a small device like a USB memory stick that can be attached to your keyring. For a successful login to your Gmail

both a password and a memory stick are needed. This might sound cumbersome but can prove extremely effective in preventing malware and email hacking attacks. Employees at well-known organisations, like Cern, Facebook and Google, use devices like Yubikey to protect their email accounts and other cloud-based services.

TOP TIP:

The usefulness of a secure password is negated if the security questions for email and other web-based services are too easy to guess. In fact, Google's research into security questions such as "What was your first car?" or "your favorite pizza topping" showed that they are "neither secure nor reliable enough to be used as a standalone account recovery mechanism" as some of this information can be gleaned from social media. Moreover, even the most secure passwords can be revealed if your Mac or Windows system is infected with keylogging malware.

My passwords are driving me to distraction. Is there an easy way to manage them?

Passwords are becoming the bane of the modern computer user's life. While there are many online password managers out there, such as LastPass, many users are still a bit apprehensive about storing all their passwords online.

You could try **KeePass**, which is a password manager that stores your passwords locally on your PC or Mac. All your passwords are encrypted with AES-Rijndael (or Twofish). Your password database is further protected by a master password (protected by the SHA-256 hash function).

Is there any way to check if my email has been hacked?

To find out if your email address has been compromised by a data breach you can visit the "Have I been Pwned" (**https://haveibeenpwned.com**) website.

Every week, this website collects information from email addresses and website accounts that have been compromised. It is an easy way to check if your private information has been leaked or compromised. It also offers a "Notify Me" service which allows you to get a notification if any of your personally identifiable information has been leaked.

Ransomware – a game changer for computer users

12 News

'Pay €300' virus hits PCs here

Adrian Weckler

A DANGEROUS computer virus that wipes out personal documents and locks sensitive files is attacking Irish computers, say security experts.

Called Cryptolocker, the so-called 'ransomware' virus demands €300 from owners of infected computers.

Once active, the virus locks all files and documents on the computer. It then demands up to €300, payable online through untraceable money wire services, to unlock the files.

"It's definitely one of the most damaging pieces of malware I've ever seen in the last 10 years," said Rob Scanlon, founder of IT security firm ComputerAmbulance.ie.

The Cryptolocker malware, which is not known to affect tablets or smartphones, is caught by opening programs in hoax banking emails or by visiting some adult websites.

The malware has been in circulation for two months, but appears to have begun infecting Irish PCs in greater numbers over the last two weeks.

Experts advise that the best way to protect against 'ransomware' applications such as Cryptolocker is to regularly back personal files up.

Not so long ago, the biggest risk to your data was probably from hard disk failure or accidental deletion, but now those risks have been eclipsed by ransomware attacks, such as the pernicious Cryptolocker malware. This malware uses 256-AES cryptography to "lock" files. The only way to recover them is by paying the ransom which can be anything from €300 to €3000. Between mid-2013 and May 2014, Cryptolocker infected more than 260,00 computers worldwide. Victims have included police departments, insurance companies and legal firms. We have seen personal computer users lose years worth of irreplaceable photos. Even businesses with sophisticated firewall appliances and dedicated IT security teams have been caught out by crypto-virus attacks.

<<

Computer Ambulance was one of the first IT companies in Ireland to issue a warning to the national media about ransomware.

Preventing ransomware

There is no foolproof way to prevent ransomware attacks. Of course, some IT security vendors (of the snake oil marketing variety) have been touting silver bullet software and hardware solutions to this problem. But, at the time of writing, there is no one single solution out there that can be guaranteed to protect your computer or network. However, by using a layered approach to your IT security, you can mitigate against such attacks and should keep you relatively safe at least. Some worthwhile precautions include:

Off-site or versioned backup – If your backup device is connected to your Apple or Windows system at the same time as a ransomware attack, it is likely that it will also get infected. For this reason, it is imperative that you use an off-site versioned backup.

User education – All users on your network must be made aware of the risks that are inherent in clicking on an innocuous looking email. Ideally, they should be trained to spot anomalies in emails and websites.

Effective spam filter – The main conduit for crypto-viruses is email. So it's important to have good spam filters that will flag the user when a particular email is spam or suspicious.

TOP TIP:

Even email attachments from known senders can be dangerous to open. For example, let's say you have a customer called ABC Consulting Ltd which is run by Pat Murray, whose email address is 'patmurray@abcconsulting.ie'. If Pat sends you an email with an attachment out of the blue, you would assume it's safe to open, right? Well, no, because if Pat's email has got hacked, the hackers can use his email address and its address book as a launch pad for phishing attacks and other nefarious activity. So it can even be risky opening emails from known senders.

I've just bought a new computer. How do I securely delete the data from my old computer's hard disk?

There are many ways to irreversibly destroy your data. For Windows-based systems utilities, such as Dban, can securely wipe your data by writing zeros to your old hard drive in accordance with US Department of Defense standard 5220.2M.

For a Mac, the secure deletion process is a little more convoluted. Firstly, turn on Filevault encryption and wait for the encryption process to complete. Then reboot your system and use Disk Utility, go to the Erase tab and format the drive to Mac OS Extended (Journaled). If someone does try to recover the data it will still be encrypted. Once your hard disk has been deleted don't forget that your Mac will store your WiFi password in it's NVRAM, so make sure that your Mac's PRAM is reset.

If your old system uses an SSD, you can download the utility provided by the disk manufacturer and use the "sanitize" function to securely wipe your disk.

Using software-based tools is not the only way. Another technique is to physically destroy your hard drive by using a hammer or a drill. This might sound a rather crude method but leaves very little room for user error. For many state security agencies, such as the NSA, physical destruction of data medium is the only form of data destruction which they deem safe.

TOP TIP:

In the excitement of acquiring a new computer system, many users want to immediately recycle, donate or dispose of their old system. This is understandable. But it is strongly advised to have a "cooling off" period first. Remove the hard disk from your system and keep it for at least six months, just in case you need any further data from it.

How do I protect my kids from explicit content on the internet?

There are a lot of "internet protection" software packages that claim to block explicit content. However, most of these are gimmicky as they only work at browser level. The best content filtering software works at DNS (Domain Name Service) level, such as the free **OpenDNS Family Shield service**. Once your router is configured for OpenDNS, all devices in your house that work off WiFi, such as laptops and smartphones, get their content filtered at source (your home router).

My data is in the Cloud, so there's no need to back it up, right?

There is a common misconception that once data is stored on cloud services, such as Google Apps, Office 365 or Gmail that it's "safe". But this could not be further from the truth.

Just because your data is "in the Cloud" does not imbue your data with indestructible qualities. Data in the Cloud (just like locally stored data) can get corrupted or accidentally deleted, or a hacker or employee could sabotage it. For example, thousands of Irish Gmail users get their accounts hacked every year and end up losing several years' worth of emails and contacts, which can be devastating.

To mitigate against this you should backup your cloud data. There is a multitude of applications available, such as **Gmvault** for Gmail or **Backupify** for Office 365, which can mitigate against data loss in the Cloud and help you to sleep a little sounder at night.

My broadband company (ISP) has told me I am subscribed to a 100Mbps line but I'm only getting 65Mbps?

Many users wonder why they are not getting the same internet speed as described on their broadband subscription package. This is because the advertised speed is normally just the theoretical maximum speed of broadband in your area. However, not every subscriber will be getting this. There are a number of reasons for this, including:

- Your distance to the nearest fibre cabinet determines your modem sync rate. Previously, your broadband speed was heavily dependent on the distance to the local telephone exchange. But now providers, such as Eir, use FTTC (fibre to the cabinet) technology which generally means that the closer you are to a Fibre Cabinet, the faster your connection will be. (These fibre cabinets are usually green or grey coloured boxes on Dublin street corners.) Inside they contain a device known as a DSLAM, which aggregates broadband lines in your area and forwards them to the rest of the network.

- Plant and cabling quality. If you're connected to a modern or recently upgraded exchange it is more likely to be using modern plant and equipment.

- User density ratio is another factor that influences both download and upload speeds. The more people who are "sharing" a connection, the slower it's going to be, especially at peak times.

- Next comes your modem. If you're subscribed to fibre-power broadband you should be using a VDSL2 modem or modem-router. If you're subscribed to a cable connection (such as Virgin) for maximum speeds (and assuming your local network supports it), your modem should support the DOCSIS 3.0 protocol.

Enjoy a reliable, far-reaching and secure wireless network

Not so long ago, most computer users were happy with wireless in one or two rooms of their house. Now with the proliferation of tablets and smartphones, users want seamless wireless in every room. For some households, this can be a challenge as they normally rely on their ISP-supplied router for coverage. This can leave some users with a lot of wireless "dead spots".

However, there are a couple of things you can try to improve the wireless quality in your house.

The first solution many users think of when trying to extend the wireless signal in their house is to buy some "boosters". There are many computer stores selling devices that claim to increase the signal coverage zone in a building. While it is true they can increase the area covered this also comes with the price of a vastly reduced throughput rate. Most of these devices take the signal from your main router and then try to retransmit it, but in doing so they halve the signal which gets sent to your endpoint device, such as your laptop, TV or tablet. Boosters sound great in theory but they are not so good in practice.

The latest generation of wireless routers: what manufacturers don't tell you

If you're in the market for a new router you will probably come across "MU-MIMO" class routers. These multi-antenna tri-band routers might look like a prop from a Star Wars film, but are in reality rather useless if you're looking to extend the wireless signal coverage in your house, as 5GHz signals don't penetrate walls or ceilings very well. However, for multiple users in an open-plan office space, then a MU-MIMO router will excel in delivering high data throughput rates.

What about the Apple Airport Express and Airport Extreme?

Using an Airport Extreme as your main router is fine, especially if your devices are primarily Apple. However, using its baby brother, the Airport Express, as a "booster" can create a bottleneck on your network as it has a speed limit of 100Mbps, Moreover, if you're using it in "wireless repeater" mode, your data throughput rate will be reduced by 50%.

The future of home and small office wireless networking

Expect to see wireless solutions for your home or office become more innovative and sophisticated in the next couple of years. Manufacturers like **Eero** and **Ubiquity** are now devising wireless mesh equipment for homes. Mesh networking, which was once the preserve of enterprise networking spaces, means that wireless "nodes" can be deployed in your home. These bounce signals off each other and offer almost blanket-like coverage. Meanwhile, companies like Roqos are introducing cloud-managed routers with built-in enterprise security features, such as DPI (deep-packet inspection) – a feature normally only seen on business-class firewalls. However, these technologies adapted for your home and small office use are still in their infancy and you are probably better off waiting until they become more refined and less expensive.

Five common Windows 10 problems and how to fix them

1) Windows 10 can no longer update

If the Windows 10 update function is not working, try running the Windows Update Troubleshooter. This will scan your PC for problems and recommend a solution if it finds any. It can often weed out issues that prevent Windows 10 from updating.

2) Fix Windows apps that crash after a Windows 10 update

Sometimes Windows apps (bought from the Windows store) will crash after an operating system update and can sometimes "break" as a result. To remedy this, press both the Windows key + X simultaneously, click Command Prompt and type "wsreset". If this does not work, go to Settings > System > Apps and Features and select the troublesome app. Then select Advanced Options and "Reset".

3) Fix problems with Microsoft Office

If any of your Microsoft Office applications, such as Word, Excel, PowerPoint or Outlook, are misbehaving you can download the Microsoft Office Configuration Analyzer Tool to help detect problems. After downloading the tool, run it and select the applications that you would like to scan. When it detects a problem, it will helpfully suggest "Download the update for this issue".

4) Windows search bar not working

This can frequently be attributed to a corrupt version of Cortana. This can be remedied by disabling and re-enabling Cortana.

5) Skype keeps on crashing

The inbuilt version of Skype that comes with Windows 10 can be very crash-prone. For a more stable version, download the latest version from Skype's main website. You will need to uninstall the older version of Skype first though (Start > Settings > Apps & Features > select Skype > uninstall).

The problem (and solution) to standalone backup drive failure

One common strategy that users employ for backing up their files is to buy an external USB hard drive and store all their important documents, pictures, home movies, etc. onto that. But if the external drive fails (which they often do) you may end up losing all your important data, so you need to hedge your bets a little.

This is where a storage concept known as mirroring comes in. Instead of just using one disk, you use a storage device with two disks inside and your data is written simultaneously to both. Now if one disk fails, you still have an exact copy on your second disk.

This sort of functionality can be got on a device called a NAS (Network Attached Storage). This device can be as small as a toaster and is a really neat way to backup data locally.

Your own server for your home or office

A couple of years ago, a NAS was merely a smart hard drive. Nowadays, a NAS acts like a mini-server (or private cloud) and most now come with their own operating system. Not all NAS devices are equal – some perform their backup and file serving duties better than others, and some are easier to use than others. Attributes to look out for when choosing a NAS include:

A number of hard disk bays – Some NAS devices only come with two disk bays which means that only RAID 0 or RAID 1 can be used. If you have RAID levels 5 or 6, which support 2-disk simultaneous failure, a 4-bay NAS is advisable.

Processor power – If you're streaming video from your NAS or working with large files, like Photoshop, a NAS with a quad-core processor is recommended. A single or dual-core processor might prove a little breathless at such tasks.

Support for Windows and Mac – Some NAS devices like Synology and Qnap devices support Apple Time Machine Backups, others don't.

Support for versioning – In the age of crypto-viruses, file versioning is important, i.e. backup sets taken at different time periods.

Cloud backup support – If you're using your NAS as a file server rather than a backup device, look out for cloud-backup support. For example, many NAS devices now support backup to Dropbox or Amazon Cloud Drive

Remote Access – If you need to log in to your NAS remotely, make sure it supports a feature known as "DDNS".

TOP TIP:

Most NAS devices do not come with hard disks pre-installed. You will need to purchase these separately. Most quality NAS devices will only accept certain models of "NAS compatible" hard disk, such as WD RED or HGST Deskstar NAS. Your NAS will not function properly if "green" or "eco-class" disks are used.

The safest possible place for your photos

There are loads of options that are available for storing your photographs, both locally and online. Storing them on an external USB hard drive is one option, but do you really trust a mechanical hard drive to be still working in 20 years time? Another option might be to use an online service like iCloud, but this is liable to hacking and your photos could be erased within seconds. Another question to think about is "will iCloud (and similar services) even be around in 20 years time?" Bearing all of this in mind, your safest option for storing precious photos might be to burn your photos onto some good quality archival-grade DVDs (such as Verbatim M-Disc) and store them in a safe place. They are inexpensive, non-magnetic and won't become inaccessible if accidentally dropped. Simple but very effective.

Should I buy the iPad Pro or just get a Macbook Air?

Deciding whether to buy an iPad Pro or MacBook Air really depends on your type of usage. There are a couple of considerations to take into account.

Storage – The entry-level iPad Pro device starts off with just 32GBs of data storage and has a maximum storage of 256GB. Many USB memory sticks can hold double that amount, while a MacBook Air has storage capacities up to 512GB. This is important if you work with large files like photos and PDFs.

File management – With the iPad Pro, your applications decide where your data will be stored; unlike the MacBook Air, where you have the freedom to create your own folders and directories.

Keyboard – The MacBook Air has a keyboard which is less fiddly to type with and feels more solid in comparison to most iPad Pro keyboards. This is important if you do a lot of typing.

Pencil – The iPad Pro comes equipped with a device known as Apple Pencil, which is the Rolls-Royce of stylus-to-screen interfaces. It is sharp, accurate and quick. Very handy if like to take notes by hand or want to use a very sophisticated digital scribble pad.

Applications – The iPad Pro is able to run an amazingly comprehensive array of apps. However, it still cannot run applications, such as Photoshop or Sage. Moreover, ROS cannot be installed on it which means you can't file a tax return while waiting for your flight or enjoying a skinny latte in Starbucks.

Using an iPad to connect remotely with your Mac or Windows PC

Everyone is familiar with that sinking feeling when you're en route to an important meeting or presentation with only your iPad and realise that a really important file is residing on your Mac or Windows PC. Wouldn't it be great to log in remotely by just using your iPad?

Now you can with **Splashtop for Business**. You simply install the app on both systems (iPad or iMac or Windows PC) and connect remotely. It allows you to view files, transfer data and even allows video streaming from the remote computer. Splashtop for Business uses 256-bit TLS end-to-end encryption that is fully HIPPA compliant.

Why you should never trust iCloud alone

Every week we hear reports of users whose data which has mysteriously disappeared from their iCloud. Other reports include users who log in to their iCloud account and discover that their data has mysteriously disappeared only for it to reappear a week later. Moreover, there are perpetual issues that surround iCloud not being able to keep all devices in sync. For example, iCloud might sync your iMac's data perfectly but then fails miserably in keeping your iPad in sync. Truth be told, web-based services are not a forte of Apple and never have been.

We're not saying that you should not use iCloud. When it works properly, it can be a lifesaver if you've lost your iPad or iPhone, but you should not trust it totally. It's always a good idea to back-up your iPhone or iPad periodically to iTunes using a USB cable. Better safe than sorry.

10 essential rules for reliable data backups

Categorise your data – Before you start thinking about purchasing backup hardware or hosted backup plans make sure that you categorise your data first. For example, backing up 2 terabytes of photos to the Cloud might be time-consuming and expensive. Whereas file types, such as Word, Excel and Powerpoint, will upload quicker and use less storage.

Centralise your data – Some backup strategies involve multiple devices being backed up to multiple locations. This usually results in a messy data sprawl which not only results in some data not being backed up, but also makes the data restoration process tedious and time-consuming (if needed). So before you rush into a data backup strategy, have a simple but clear plan of what devices need to be backed up, and where they will be backed up to.

The best backup systems are automatic – Backup systems that require a lot of human intervention run the risk of being unused because many users have a habit of relegating the backup function to the backburner. This is why the best backup systems use scheduling so that they can run automatically in the background, which means minimal human intervention is needed.

Backup applications are not all created equal – As with any software, there are good and not so good backup applications. Some are robust and execute the backup function reliably, others can be glitchy and temperamental.

Complexity elevates the risk of error – Some backup applications present the user with multiple permutations of backup options. This might sound great in theory, it just increases the risk of human error in practice and the risk of the backup process not running at all. There is a lot to be said for the simplicity of software like Apple's Time Machine.

Always verify your backup – Backups need to be verified every so often. Good backup systems will allow you to verify your data both quickly and easily.

Off-site backup is important – Dublin might not be in Tornado Alley and does not have to endure weather extremes, but the risks of fire, flood, burst pipes, theft and sabotage are ever present. This makes off-site backup extremely important.

Backups can be destroyed by ransomware – Cryptographic ransomware can destroy backups in a matter of seconds. This is why your USB attached or server backups should be isolated or air-gapped after a backup has been successfully completed. If you're using applications that synchronise data to the Cloud, such as Dropbox, make sure that the file versioning functionality is enabled.

You need a "backup of a backup" – Just because your data is in "the Cloud" does not mean that it's safe. Even the most sophisticated and modern data centres have been known to corrupt or lose data. Moreover, employee sabotage and hackers are other risk factors that can make cloud-based backups vulnerable.

Backup systems need to be dynamic – Most modern IT setups are fluid, as users change devices frequently, and so their requirements also change. Good backup systems can be re-configured to easily accommodate these changes.

Avoid having your data compromised when you use public WiFi services

Wi-Fi hotspots have now become ubiquitous in cafes, bars, airports and hotels, as well as on board public transport. These hotspots are normally faster and more economical to use compared to the 4G internet on your phone or tablet, especially if you're roaming abroad. However, this can come at a cost of less security. Every time you log on to a Wi-Fi hotspot your data is at risk of being "sniffed". This means that your online banking details, credit card details or email passwords could be accessed by a hacker. However, there are a couple of steps that you can take to minimise the risk of your data being compromised when using public Wi-Fi.

Always make sure that you're logging on to the official Wi-Fi of the venue or location where you are accessing the internet. For example, if you're staying at the Hilton Hotel, use the official guest Wi-Fi SSID, which might be called "Hilton Guest". Do not be tempted to login to any other SSIDs, such as "Free Wi-Fi" or "Hotel Wi-Fi", as these could be rogue access points set up by the local friendly hackers.

While most "secure" websites already use SSL encryption, a hacker will still be able to see your data traffic. To mitigate against this, you can use a VPN service, such as Vypr (available from **www.goldenfrog.com**), which encrypts all of the data from your browser to its destination. This protects important data, such as your online banking logon details. Once installed, it is always good practice to wait until the VPN link is fully initialised before accessing your Gmail, email client or any other secure sites.

Useful Apps and Services

WeTransfer – Ever needed to send a large file to somebody without having to mess around with Dropbox permissions? Now you can with WeTransfer. It's free, secure and fast.

Pocket – Ever come across interesting content on the web that you would like to access later? Using "favourites" or "bookmarks" in your browser can be convenient, but it can become messy if you're using multiple computing devices. Using the Pocket utility, you can save and access links, articles, videos or webpages to a Cloud-based account with just a single click.

Sophos Anti-Virus – A nice free anti-virus package for Apple Macs without causing a performance hit.

Ghostery – Nice browser extension for Chrome, Firefox and Safari that tells you which websites are tracking you on the internet.

Coconut Battery – App which tells you about the health of your Macbook or Macbook Air's battery.

Scanner Pro – Turns your iPhone or iPad into a portable scanner. Makes scanning receipts, books and magazines easy. Helps you to get one step closer towards that elusive paperless office.

Inbox – A neat app for Gmail users which allows you to set-up a to-do list in your email account. It also enables you to see your order updates, flight status and pictures without even opening the message.

Trello – This app is the closest you will find to having a virtual whiteboard on your phone, tablet or PC. It allows you easily track ideas, goals and task progression in an intuitive, easy-to-use interface.

F.lux – Staring at your Mac's screen all day can take its toll on your eyes. F.lux adjusts the colour of your monitor based on the time of day, so that your eyes can get a much-needed break.

Slack – Email as a communication tool is not as efficient as some people think. A nice alternative is Slack. Dubbed by some as "the email killer", it has over 3 million active users worldwide and can offer a leaner way for groups to communicate with each other. .

Contact Us
It's Good to Talk

We hope that you have found this edition of our Essential Technology Guide useful. Whilst we have tried to cover as many topics as possible, it presents only a tiny snapshot of what Computer Ambulance does.

If you would like further information on a specific I.T. related issue and need a solution, or you simply just need a computer fixed - **call us on 01-685 4838**. We're here to help (and our phones are answered by real humans).

Computer Ambulance, Dublin

www.computerambulance.ie
T: 01-685 4838

Computer Ambulance is part of the **Mizen Group**