A Brief Rundown on Malware

Howard Houliston

Contents

Introduction

The intended audience for this publication is the general public, not security experts – they will already know everything that is described here. Although I worked for many years as an IT specialist it was never in a security related role. But I know enough to know that malware is a subject that most people don’t know enough about.

People are not allowed to drive unless they demonstrate sufficient competence and obtain a licence, yet anyone can own a computer and, by not being sufficiently aware of the dangers of malware and how to manage the risks, put themselves at risk of various types of attacks, with possible serious financial consequences.

So this is not needlessly complex and technical, it simply sets out to describe the nature of malware, and how to reduce the risk of being adversely affected by it. I hope you find it understandable and useful.

Howard Houliston

What is Malware?

The term ‘malware’ is short for ‘malicious software’ – it is software which somehow gets installed without the knowledge or consent of the user of the computer or device, and it does things which the user would not want to happen.

It’s a very broad term which covers highly malicious items like ‘ransomware’ (where files on your device are progressively encrypted in the hope that the user will pay a ransom for them to be decrypted again) as well as much less harmful activities like working to present unwanted advertising.

It’s hard to argue with the conventional wisdom that you should try to stop malware being installed in the first place, and if you discover any then you should get rid of it. Although there is general agreement on those two points, there are many different opinions on HOW you should go about doing those things.

Malware can be present on many different types of computers, not just Windows PCs. Apple desktops and laptops, Linux computers, Android tablets and phones, as well as Apple tablets and phones are all essentially computers that can be targeted by malicious software. In this publication the term ‘computer’ includes all of these devices.

To guard against malware, it’s very helpful to know about the different types that exist, how they spread and what they do.

So here’s a brief run down on the different types as well as a brief explanation of some related terms:

A Brief Rundown on Malware

Viruses are the type of malware of which most people became aware first. A virus is self-replicating and is always imbedded in some other program or application. An application or ‘app’ is a type of program; when the term ‘program’ is used here, it includes applications. When the program that hosts the virus is started, the code in the virus is also run, and in the process it will look for means whereby it can spread. It will also do whatever the virus was designed to do in the first place, possibly ransomware activities, maybe collecting personal information or perhaps just getting up to mischief and messing up your system, it depends on the virus.

Worms are very much like viruses except for one thing: a worm does not imbed itself in a host program, the worm is a stand-alone program which is capable of self-replication. For example a worm might access your address book and send itself via email to all of your contacts.

Trojans are named after the wooden horse used by the ancient Greeks to get into Troy. They are generally stand-alone programs which appear to have a legitimate purpose, but unknown to the user they are also carrying out some type of malicious activity. They are not self-replicating.

Bots are not always malicious. Examples of ‘good’ bots are those which do web crawling to gather information for search engines, or those involved with instant messaging. One type of malicious bot is self-replicating malware which infects a computer and connects back to a command and control centre. The term botnet refers to the control centre and all of the infected computers it connects to. A system like this might be used for a denial of service (DoS) attack on a website of the controller’s choosing – computers all over the world are commanded by the controller to bombard a particular web site with traffic, so that it becomes unusable.

Malicious Rootkits embed themselves in the operating system kernel. By modifying the behaviour of the operating system many types of unwanted activity can be facilitated. A hacker can secretly access a computer infected with a rootkit. Rootkits can be used to install additional malware onto a computer. They can be used for keystroke logging to discover passwords so that hackers can access your password protected accounts. By modifying the information returned by system calls they can be used to prevent other malware from being detected. Rootkits themselves can be extremely difficult to detect, as well as being difficult to eliminate. Sometimes the only way to confidently remove a rootkit is to reinstall your computer’s operating system, and even then, that might not be enough (if it’s a ‘firmware rootkit’). The technology employed by malicious rootkits can also be used intentionally in a non-malicious way, so not all rootkits are necessarily malicious.

Sometimes a computer or device can be infected by a coordinated combination of different malware types, this is known as a Blended Threat.

A Zombie is not a type of malware, rather the term refers to a computer which has been infected (often by a malicious bot) so that it can be called upon to take part in malicious activity such as a denial of service attack. Other unwanted activities a zombie computer might perform include sending spam emails to infect other computers, or hosting contraband data like child pornography. Typically the user of a zombie computer is unaware of the infection, and most of the time notices no performance degradation or other evidence of malicious activity.

Once again, a Back Door is not a type of malware, it is an undocumented means of accessing a system, possibly without the need for a userid and password. A back door can exist because of an oversight in the design of the system, or it could have been intentionally created by the system designers, or it could exist as a result of system modification by malware.

An Exploit is the term for taking advantage of a weakness or vulnerability in software to carry out malicious activity, quite likely putting multiple malware items onto your computer.

Badware is an umbrella term that includes malware and more, it basically refers to software that disregards your choice as to how your computer or network connection is used. The www.stopbadware.org site has been associated with various US universities, initially Havard and now the University of Tulsa. As an example, software could qualify as badware if it quietly installs one or more unannounced products at setup time, but does not remove them if you uninstall the main software item.

Spyware gathers information on the computer user without their knowledge. This could be for targeted advertising purposes, or something altogether more sinister, like collecting information to access your finances.

Adware is software designed to present advertising, or to collect information for purposes related to advertising. It is not considered to be malicious if it does this with your consent, but often this is not the case.

Malvertising is advertising with hidden malicious content intended to infect your computer or device with malware.

Scareware creates the perception of a threat, generally to induce the purchase or installation of some software which would otherwise be of no interest to the computer user. It might offer a free scan of your system, pretend to do a scan, and then say you have hundreds of problems, so you’d better download this dodgy product to fix things.

Ransomware is malware that demands a payment to restore normal functioning of your computer. Commonly your files will be encrypted so that they are unusable until you pay a ransom to get a key which it is claimed will decrypt your files (the key usually works, but not always).

Phishing is the practice of sending email with a link to a phoney sign-on page, intended to lure you into entering your sign-in id and password on that page so that they can be captured by bad guys who can then use them to access your account. Never click on links in an email that seem to be intended to take you to a sign-in page, especially the sign-in page of a financial institution or any site that contains sensitive data.

Terms such as Greyware and PUPs (potentially unwanted programs) are sometimes used to describe low-impact malware, for example adware that subjects you to more advertising.

Viruses, worms, Trojans, malicious bots and malicious rootkits are the basic types of malware. Things like ransomware and spyware incorporate one or more of these basic types of to carry out their unwanted activities. As well as being aware of the different types of malware we also need to be aware in more detail of what it can do.

What Malware can do

If we are going to guard against malware, we should know what we are trying to prevent. The impact of malware can range from mild annoyance (e.g. unwanted advertisements) to catastrophic (e.g. accessing your bank accounts and emptying them of money). Here are some of the possibilities:

It can find personal information. Even if you imagine that there is no personal information on your computer or device, that's probably not the case, for example:

- You most likely have some sort of address book with contact information for your friends; malware on your computer or device could result in your friends being put at risk by being the recipients of infected emails.
- There is quite likely personal information in the emails that you have.
- Sometimes browsing history can reveal a lot.

Once a hacker has enough of your personal information they are in a position to do things like opening a credit card in your name, or worse still accessing your financial accounts and robbing you. Personal information should be protected.

Malware can simply carry out mischief. The author of this type of malignant software does not want anything from you, they just get some sort of twisted satisfaction from knowing that they are being a nuisance. The mischief could take the form of wiping everything from your computer (that's serious mischief) or something relatively innocuous like popping up strange messages on April Fool's Day. This type of malware was, in relative terms, more common a few years ago. In recent times there has been more focus on malware that delivers some sort of benefit to those who produced it.

Malware can use your computer or device to carry out a Denial of Service (DoS) attack. A denial of service attack on a website refers to the situation where thousands, perhaps millions, of computers all attempt to access the site at the same time. The site is overloaded and legitimate users cannot access it. But buying millions of computers to do this is obviously not practical, so those preparing for a DoS attack go about it by infecting millions of computers around the world with malware, which for the most part exists quietly on a 'zombie' computer or device, just waiting for the command from the controller of the botnet to which all of the zombie devices belong. This type of malware is likely to do the infected PC (they are usually PCs) no harm at all, so that the owner suspects nothing and is not motivated to seek out and eradicate the infection.

The term 'The Internet of Things' (IoT) refers to the internet connections from electrical devices that you might have around the home, things like CCTV cameras. As another example, a pump connected to a swimming pool might have an internet connection; the purpose of this is to generate alerts when sensors detect problems. A description of the problem and the serial number are sent to the manufacturer, who can look up the serial number to see who the pump is registered to and then send the pump owner an email describing the problem. Because the devices connected to the Internet of Things generally contain absolutely no personal information, there has been little concern with security. This makes them easy targets for malicious bots looking to add devices to a botnet for use in a denial of service attack. This is not conjecture – it has already happened.

Malware can use your computer to send out spam emails to other people in an attempt to infect them too. This is another example of what a zombie computer might do, against the wishes of its owner. But it's not just zombies that are likely to do this; a straight forward Trojan infection might also do the same.

Malware can use your computer to store contraband data such as child pornography. Yet another example of what a zombie computer can do, not a very nice thought, but fortunately this sort of thing doesn't happen too often.

Malware can encrypt your files and demand that you pay a ransom to regain access to them. In this situation you have several choices:

- Pay the ransom – often this works but not always. Paying up is generally seen as a bad move – if nobody ever paid the ransom then the bad guys would stop propagating ransomware.
- Remove the malware and restore your encrypted files from backups that you have. This is the best approach if you can make it work. I have seen instances where a scan by the installed anti-virus product fails to remove the ransomware, but a one-off scan from the free version of Malwarebytes succeeds. After the malware has been removed, check that all applicable operating system updates have been applied (if you have been infected there's a good chance that you were not up to date) and then restore from your backups.
- If you can't remove the malware, or if you think that your system is in a bit of a mess anyway, you might want to consider re-installing the operating system (e.g. Windows, MacOS or maybe iOS for iPads and iPhones). After re-installing and applying all available updates, restore your data from backups. This is a bit of a drastic solution, but is likely to give you a nice clean system.

Unless you decided to pay the ransom, you need backups of your data to resolve the situation. Some types of backups may not be good enough – for example if you rely only on there being a copy of your files in cloud storage (i.e. you are using Dropbox, iCloud, Microsoft

OneDrive or similar) you may find that the files have been copied to the cloud after being encrypted.

Malware can cause you to be subjected to more advertising than would otherwise be the case. This is annoying, but way less serious than some of the other effects of malware.

One of the objectives of some types of malware is to find the userid, and more particularly to find the password associated with your financially significant accounts, like online banking. Your online banking password should always be different from the passwords of other non-financial accounts – this is important. Because if, for example, Yahoo gets hacked so that bad guys know your Yahoo password, and if that password is the same as your online banking password, then the bad guys also have your online banking password. Not good.

Before going on to discuss how to guard against malware, the different types of people or organisations producing malware will be considered.

The Producers of Malware

It seems that there are three main sources of malware: pranksters, cyber-criminals and governments.

Of these, most people would consider cyber-criminals to be of the greatest concern, but the role of governments in this understandably worries many people too, especially if there are human rights issues.

The information released by Edward Snowdon suggests that the American NSA had implanted malware on something like 85,000 to 100,000 computers and devices. It's generally believed that you have to be an extremely attractive target for this to be of real concern to you, but no one likes the thought of their computer being infected with government spyware.

Of more concern are the side effects of this government activity. As well as developing its own malware products, the American government is believed to be one of the major purchasers of malware and information on operating system vulnerabilities. There is a risk that if the government just sits on this information, especially operating system vulnerabilities (rather than contacting the providers of the operating system so that they can come up with a fix) then cyber-criminals may somehow access the same information and use it to build their own malware.

This is what appears to have happened with the WannaCry and Petrwrap ransomware malware in mid-2017, both of these use the exploit known as EternalBlue to infect Windows machines via a malicious bot. The NSA knew about EternalBlue but chose to keep it as a weapon in their cyber-arsenal rather than tell Microsoft about it. Microsoft eventually found out about the exploit and corrected the operating system weakness in March of 2017, so that by the time WannaCry struck the only people affected were those who had not kept their Windows Updates current. But there were a lot of people in that category unfortunately.

It seems that these two instances of ransomware can spread in more ways than just the malicious bot, for example the speed camera network in Victoria Australia, which is not connected to the internet, became infected. A USB memory stick used for maintenance purposes is thought to have been responsible.

Protecting Classic Computers

What needs to be done to protect against malware? Can you just buy a good anti-virus product, install it and then not worry about anything? – NO!!!

Without wanting to discourage the use of good anti-virus products, it must be said that you need to do more than that.

The best two things that can be done are to keep your operating system up to date, whether it be Windows, macOS or Linux, and to be aware of what behaviour is dangerous when using your computer.

It may take up to thirty days between the introduction of new malware and anti-virus products being updated to combat it.

Anti-virus products employ something called 'heuristics' – which means that if something looks like malware, even though it isn't in their malware definition database, they will treat it as malware. The problem with heuristics is how to stop all new malware without incorrectly identifying innocent software as being malicious (which is known as a 'false positive'). The harder you try with heuristics to stop everything that might be malware, the higher the chance of a false positive.

More than anti-virus software is needed. Avoiding behaviour that puts you at risk is a good start.

If you see a suspicious looking email in your inbox it's probably best to delete it without opening it. If you are tricked into opening it, and see a link in the email, on no account click on the link; this is probably an attempt at phishing (as described earlier) or it could take you to a page with malvertising.

If it's easy to do, check the sender's email address. It's increasingly common for email software to only show the sender's name without showing the email address, but the email address can sometimes be found by things like a mouse-over on the name, touching the name if you are on a touch-screen, right-clicking the name or left-clicking the name if you have a mouse. So if you get an email claiming to be from your friend Fred Smith, whose email address is fredsmith@foo.com, but you manage to see that the sending address is really something like 1$77@731mail.com or even fredsmith@731mail,com then you can be sure it's a scam, probably part of an attempt to infect your computer or to trick you into entering password information. Delete the email instantly.

Malvertising can be sinister. Sometimes, if the circumstances are right (or wrong, depending on your viewpoint) the associated malware can even be installed without you even clicking on anything. Free porn sites are possibly the category most heavily infected with malvertising, but there can be malvertising on reputable sites too. Avoid the bad effects of malvertising as best you can by minimising or totally avoiding clicking on advertisements (particularly ones that seem to offer something too good to be true), by keeping your operating system up to date and by keeping Adobe Flash Player up to date as well, if you have it installed.

The common sense rule applies – if something seems too good to be true it probably is – leave it alone.

OK, we know to keep our operating system and other important software up to date, we know to avoid suspicious emails and suspicious advertising, but what should we do about anti-virus software? (It should probably be called anti-malware software, because of the protection offered against Trojans, worms, rootkits and so on, but the term anti-virus seems to have persisted) Do different rules apply to Windows

PCs, MacBooks and Linux PCs? Should a free anti-virus product be used? Is it worth spending money to try to get something really good? Or, if it's a Windows PC, is it OK to simply use Windows Defender, a part of Windows 10?

Anti-virus products are still heavily focussed on Windows. It's not that Windows is an innately much less secure operating system that needs protection more than macOS or Linux, it's because not so long ago Windows was almost the only operating system used by most of the general public. Mmalware writers probably honed their skills on Windows and tend to keep on doing what they've always done, and this makes sense since Windows still has a big market share.

Many macOS and Linux users do not use anti-virus software, claiming that they don't need one because they are using a superior product. And generally they don't seem to have any problems, but this probably results from keeping their software up to date and sensible online behaviour, coupled with the smaller quantity of malware targeting their systems. The claim that, as far as security goes, they are using a superior product would have been true twenty years ago, but Windows has tightened up a lot since then.

Pretty well all anti-virus providers offer a version of their product that runs on Windows, many offer versions that run on macOS and a smaller number offer a version that runs on Linux.

So let's consider Windows anti-virus software first, similar considerations apply to the other two operating systems.

Firstly let's look at the difference between free and non-free anti-virus software. Often the same software provider offers both free anti-virus software, as well as a version that you pay for. Why would a commercial software provider give away anti-virus software? Some possible reasons are:

- To get you as a user, in the hope of persuading you later on that you'd be better off with the pay-for version.
- To make money from you by presenting advertising. Anti-virus software like this cannot be called malicious adware, since the user agrees to the advertising in accepting the terms and conditions.
- To change your browser's default search engine to one of their own, probably with a name implying that the searching is done securely. Although they make all sorts of claims related to security, the reality is likely to be that they want to make money when you click on the advertisements that are presented with the search results.
- To install one or more additional programs by default when the anti-virus is installed. You probably don't want these programs, but the anti-virus provider gets paid if you install them.
- To track your browsing. It would then be possible for them to sell this data, maybe some or the smaller and dodgier providers do.
- There is one free anti-virus product that stands out as having none of the negative attributes described above – that's Microsoft's Windows Defender which comes as part of Windows 10. In so many ways this seems like an excellent choice – none of the negatives listed above, it is kept up to date as part of the Windows Update process and the overheads are low. So why would you use anything else? Here are some possible reasons:
- In a corporate environment a corporate version of an anti-virus product tends to be chosen to enforce the company's anti-virus policy on all users. There is no corporate version of Windows Defender.
- Some anti-virus testing suggests it is a less effective anti-virus product than the best commercial ones, especial with respect to heuristics. Microsoft tend to dispute this, often claiming that the

testing environment is skewed against them. Maybe the truth is somewhere in between.

- Although Windows Defender generally has low overheads, it can impact performance more severely than some commercial products when it is doing a scan.

But getting back to comparing free and pay-for versions of anti-virus software, as an example let's take a look at AVG (as at mid-2017) which is a popular and well regarded choice for both types of anti-virus. The pay-for version offers four additional features:

- Secure personal folders with an extra layer of ransomware protection
- Keep hackers away with Enhanced Firewall
- Avoid fake websites for safer payments
- Includes unlimited AntiVirus PRO for Android™

Let's look at the first three of these points, since the fourth has nothing to do with protecting classic computers.

The extra layer of ransomware protection for personal folders is achieved by only permitting designated programs to open the files one of the personal folders. So presumably Word is allowed to open documents in your Documents folder but an unknown program with a strange name is not. This is a nice-to-have feature, but one that mitigates the impact of a malware infection rather than preventing the infection in the first place.

The enhanced firewall is for use instead of the Windows firewall. The Windows firewall is generally considered to do a great job of stopping unwanted inbound network traffic, but it does not attempt to regulate outbound traffic. So for example, spyware sending information back to its evil master is not troubled by the Windows firewall, but may be blocked by a third part firewall such as the AVG enhanced firewall.

Once again this is a nice-to-have feature that mitigates the impact of a malware infection rather than preventing the infection in the first place.

Avoiding fake websites for safer payments is achieved by giving you use of AVG's DNS (Domain Name Server) rather than the DNS you are already using. A DNS is a server external to your home setup which translates internet addresses in name-format (like www.mysite.com) into an IP address format (like 100.200.210.220).

If a hacker gains access to a DNS they can change the IP address associated with, say, your bank's website so that people intending to go to your bank's website are instead sent to a fake site which looks identical. Once you have entered your login-id and password there the hacker knows how to access your online banking.

AVG seem to be suggesting that their DNS server is better protected against hackers than the server you would otherwise be using, something which seems hard to prove or disprove.

So you get something for you money if you go for the pay-for product, but the extra features that you get would appear to mitigate the effect of a successful malware attack, without doing anything more than the free version does to prevent infection in the first place. One benefit of the pay-for version, with anyone's product, is that you will never get nagging advertisements urging you to upgrade to the pay-for version.

Can there be a downside to using the pay-for version rather than the free one? Apart from the obvious consideration of cost that is. Yes there can be, two things in particular:

- Sometimes the extra facilities provided by the pay-for version will consume significant computing resources, making your system slower with the pay-for version. This sort of behaviour varies from vendor to vendor.
- Depending on the design of the product, you run the risk that if you fail to renew the annual subscription in time, you will have

no anti-virus software that works; the product you paid for has expired and does not work, but its existence on your computer prevents Windows Defender from becoming active.

Whether you should choose a free or pay-for version, and which product to choose, depend on many things – the types of risks inherent in your pattern of use, the power of your PC, the state of your finances, how many PCs you have to protect and so on. And the best solution in July may not still be the best solution in September – anti-virus software and pricing is forever changing.

A reasonable solution for someone cash-constrained might be to choose a free anti-virus that seems to have the required features and which current reviews indicate does not consume excessive resources, and to also install the free version of Malwarebytes.

Malwarebytes is an interesting product, earlier versions were promoted as being suitable to install alongside your existing anti-virus software, but now it claims that it ‘Makes Anti-virus Obsolete’ and looks very much like an anti-virus product. The free version does not actively protect against malware, it can only scan for and remove malware, but it does that very well, sometimes better than anything else it seems.

The discussion has been about Windows PCs, because that’s where all the action is as far as ant-virus software is concerned. But much the same considerations apply to macOS and Linux computers (though not Android or Apple tablets or phones), except that there are fewer products to choose from (especially with Linux), the amount of malware targeting these systems is much less and many users decide not to bother with anti-virus software. If you choose not to run anti-virus software on your Mac or Linux, be sure to keep your software up to date, especially the operating system and (if it is installed) Flash Player.

And don’t visit dubious web sites.

Free Public Wi-Fi

Free public Wi-Fi can be attractive, but there are some things to be wary of. A public Wi-Fi network in a sense is a noisy place, devices everywhere are ‘shouting’ and they are all able to ‘hear’ each other should they choose to. Things work smoothly because devices only respond to packets of data that are meaningful to them. But a bad guy on the network can use this as an opportunity to view all of the traffic going to or from your device, hopefully your sensitive data like sign-on ids and passwords are protected by the same sort of encryption that https uses in browsers, but with apps on smartphones and tablets it’s harder to be sure. And https style encryption may not be enough on a free public Wi-Fi network (more on this later).

One solution is not to use free public Wi-Fi, easy to do on a phone or tablet with a SIM card, if you have network coverage and a plan with a sufficiently generous data allowance. But that’s not everyone.

And a further danger is that bad guys might set up their own alternative free public Wi-Fi so that they have even more opportunities to exploit those who use it. For example the Downtown Mall might offer free Wi-Fi called ‘Downtown Wi-Fi’, a bad guy could go there and set up an alternative free Wi-Fi, which could easily fit into a back pack, calling it ‘Downtown Fast WiFi’. This puts them in a position to set up a ‘Man in the Middle’ or MITM attack on those who use ‘Downtown Fast Wi-Fi’.

If you are a victim of this, the bad guy who set up the MITM can see data protected with https-style encryption. And if it’s Wi-Fi provided by a small café for example, it may have been set up by the bad guy who runs the computer shop next, so that you are subjected to a MITM attack even if you check that the name of the Wi-Fi network is correct.

A VPN (Virtual Private Network) is probably the best way to protect against your data traffic being viewed by others, as well as protecting against Man in the Middle attacks. A VPN provides an encrypted means of point to point data transfer, and is sometimes likened to a ‘tunnel’ between those two points. One point is your device or computer, the other end of the tunnel is a VPN server, probably located in a country of your choosing. If you simply want to secure network traffic to and from your device at the local Australian shopping centre, a VPN server in Australia would be suitable as the end point of your ‘tunnel’. But if you want to circumvent geo-blocking to access, say, the US version of Netflix, you would choose a VPN server in the US. From the other end of the VPN tunnel, your network traffic flows to and from the internet site you were trying to reach in the first place.

There are many considerations in choosing a VPN. Most importantly don’t choose a free VPN from an obscure provider, since there is a risk that they provide the service to be able to access your personal data.

VPNs can use several different protocols to carry out the services they provide, and using a suitable protocol is important. PPTP is an old protocol which is relatively easy to hack, and it should be avoided. OpenVPN is the most secure protocol at present, with L2TP/IP being in between the other two in terms of security.

If the VPN plan you are considering can be used on multiple devices, read the fine print and see how many devices can use the VPN simultaneously. Some plans permit the VPN to be used from multiple devices, but only one device at a time.

If you decide to use a VPN to protect your device when using free public Wi-Fi, don’t use the VPN all of the time, since it imposes some overheads and is quite likely to be noticeably slower. Some VPNs attempt to work out automatically whether they should be on or off, if you decide on such software be sure to learn what those rules are

Tablets and Smartphones

Android and Apple tablets and phones are intrinsically less susceptible to malware than classic desktop computers, largely because each app runs in its own little world, cocooned away from all of the other apps. The Android market is dominated by Samsung, but the same security considerations apply irrespective of the manufacturer. This chapter deals with Apple and Android phones - if you have a Windows phone it will be running some version of Windows, and the considerations discussed in the chapter on classic computers apply.

One of the things we know to be wary of is a free public network, but what other points are there to consider to help make your device more secure? Many of them are quite simple, such as:

- Don’t lose it! A simple enough idea but nevertheless very important. If you do lose it, make it harder for the thief or finder to access your data by at least having some sort of unlocking process like a PIN, and in your phone settings select a short to moderate time interval for the phone to lock automatically after inactivity. Be aware that if your phone is an Android it may have a removable SD card where there is unencrypted data. Law enforcement organisations and organisations like the Australian Tax Office are understandably much more skilled at extracting data from a phone in their possession than the average person who has found or stolen your phone. There are devices called ‘flasher boxes’ and more specialised equipment that can help to extract information, even from a protected phone. An Israeli company called Cellebrite specialises in helping law enforcement organisations to do this.

- Protect your phone or tablet with some sort of PIN or password, or even a fingerprint. The fingerprint is considered less secure since you probably have your fingerprints all over the phone, but it's far more secure than nothing at all.
- If the device is an iPad or iPhone, take the time to set up the 'Find my iPhone' function, which can help to locate a lost device. It also allows you to set a lost device to 'Lost Mode' which tracks the device, locks it, and can display a message on the screen (maybe suggesting a number to ring). More recent versions of Android have a similar function known as 'Find your Phone'.
- Consider two-factor authentication for your Apple or Google account. The basic idea of two factor authentication is that a userid - password combination is not enough, more is needed. The something extra might be a randomly generated code sent to your other devices as a message. Two factor authentication may give you the option of using a trusted device as the 'something extra' so that logging on is not too troublesome. Not surprisingly Apple sometimes send numeric codes to your other Apple devices when supplementary authentication is required, so don't set up two factor authentication just before an overseas trip where you take your iPhone but leave your iPad behind. You may find your iPhone demanding the entry of a code sent to your iPad, which is in another country.
- Don't 'jailbreak' your iOS device or 'root' your Android phone or tablet. These terms refer to the elevation of the level of privilege with which apps run, so that they have greater power of access to the contents of your device. This permits nerdy users to do more things, but also creates a much more fertile ground for malware.

There are anti-virus products for smartphones and tablets, more for Android than for iPhone and iPad. The architecture of Apple's iOS operating system not only makes it difficult for virus-like malware to function, it also makes the creation of worthwhile anti-virus software difficult. The occasional operating system vulnerability is addressed by corrected software in the form of the next release of iOS.

Google also claim that their Android operating system does not require anti-virus software, although the internals of Android are not quite as restrictive as iOS, making it possible for plausible anti-virus software to exist for Android.

Android phones and tablets are vulnerable to malware though. One example is HummingBad, which might get onto your device when you visit an infected web site. This malware generates revenue by making it appear that you have clicked on advertisements and downloaded pay-for apps. It also collects personal information, which is likely to get sold. The interesting aspect of this malware is that it appears to be the product of an otherwise legitimate Chinese company called Yingmob.

Hummingbad can be detected by doing a malware scan using products from companies like AVG, Avast, Lookout or Zone Alarm. But removal, unfortunately, requires that you do a ‘factory reset’ of your device.

A lot of Android anti-virus software comes bundled with additional features which are very worthwhile if your phone is lost or stolen (which many consider to be a greater risk than malware). Some Android anti-virus products offered features similar to Apple’s ‘Find my iPhone’ prior to that sort of functionality being incorporated into Android.

So in spite of the fact that Google say that Android devices don’t need anti-virus software, it might not be such a bad idea to install it.

The greatest chance of malware getting onto your Android device is likely to be when apps are installed from places other than the Google Play Store. (Even so, apps in Apples ‘App Store’ are generally thought of as being better vetted for malware than the apps in the Google Play

Store). When installing an Android app, be wary of those that request permissions that they don’t seem to need – a flashlight application that wanted to access your contacts would be very suspicious for example. Stealing personal data is probably the most common unwanted effect of malware on phones and tablets.

Be aware that an old phone or tablet may be forced to use an old version of the operating system (Android or iOS) and as a result may be less secure than a newer device.

This especially applies to Android devices; often the manufacturer does not offer the option of going to a more recent version of the operating system. Nexus and Pixel branded Android phones are better in this regard, from time to time encouraging Android version upgrades, but other brandings tend not to do that for most of their phones.

It took longer until normal users of iPhone or iPad were assaulted by malware, but it happened. AceDeceiver appeared around February 2016. The malware needs to first infect a PC and it then can infect an iOS device connected to that PC. This particular malware appears to only affect users in mainland China.

There is less iOS malware than Android malware, and a higher percentage of iOS malware appears to be of the type that attacks and monitors political dissidents and others of interest to governments. In appears to take more effort to produce iOS malware.

An example of iOS malware is Pegasus, which first uses exploits to jailbreak the device, after which malware is installed. This is spyware believed to have been built by the NSO group and sold to governments. The exploits which enable Pegasus to successfully infect a device were fixed by Apple in version 9.5.3 of iOS. You can download a free app called Lookout from the App store to check for infection by Pegasus, as well as many other vulnerabilities or instances of malware on your system.

Apple encourages iOS upgrades. With an older device, eventually you will reach a point where you cannot run newer versions of iOS because of hardware limitations. As at mid-2017 the latest version of iOS was one of the releases of iOS 10. An older device that cannot support iOS versions above version 9 could not be more up to date than iOS 9.5.3, released in August 2016, however Apple may release a version 9.5.4 or 9.6 in the future should it be needed to correct a major vulnerability that is yet to be discovered. If one of those versions of iOS does get released, and you are on iOS 9.5.3, it would be a good idea to upgrade without delay because it would surely be correcting a major vulnerability

Conclusion

Above all else, keep your operating system software up to date.

For desktop computers and laptops, choose an anti-virus software approach which is suitable for your needs, as described earlier.

Don’t fall for scams, especially phishing scams, and remember that if something seems too good to be true it probably is – don’t get sucked in!

And avoid using free public Wi-Fi, or if you must use it, take precautions as already described.

For Android and iOS get all of your phone and tablet apps from either the Google Play Store or from Apple’s App Store. Consider anti-virus software.

May your computers and devices be free of malware!