How you can protect your computer and mobile devices from malware and data theft

Haider M. al-Khateeb

Rationale
Security specialists tend to advice that you install security tools and adapt to a list of safe-use guidelines to protect your personal devices, this is especially important when you are targeted, such as in the case of cyberstalking. Typical questions you might still ask include: how can I select a good security product for my device? Do I need an anti-virus for my phone? And what security features I should be aware of to keep my data secure?

This chapter aims at helping you answering these questions and encourages further research and security awareness on how you should use your devices. Many examples are given to demonstrate features of a particular device, but expect minor differences between different versions of a single operating system (e.g. Android). However, all the features shared in this chapter should be available in all recent versions.

Why is it important that you have an internet security product installed in your device?
A threat is a given circumstance with potential to cause harm through an attempt (attack) to breach the security of your system. In the case of your computer or mobile device, these attacks can steal or damage your data, they are triggered by numerous forms of viruses and malware that cannot be identified and quarantined without help from specialist software.
Moreover, a security package could work at the service level, they can add extra protection to your browser, prevent spyware and display warning alerts when you attempt to access a malicious website.

What threats do you need protection from?
The following threats are usually mentioned in the description of most security products on-offer, it is therefore important that you have a brief yet good understanding of what they are to help you facilitate an informed decision while selecting effective countermeasures, have a better understanding of -at least- the critical warning alerts displayed by a security product and finally, to realise the security features you need in order to protect your device.

Viruses and worms
Software designed to perform malicious acts and cause disruption to a targeted operating system. Worms are viruses but they differ in the way they spread and hide between devices.

Malware
A generic term, an umbrella that can be used to describe any malicious code such as viruses, spyware and trojans.

**Adware**
Malware designed to enforce unwanted advertisements into your screen or redirects your browser to selected websites, some are also designed to collect marketing data.

**Spyware**
Malware designed to collect data about a targeted machine without user knowledge, this can include anything from what the user types on the keyboard to visited websites and screenshots.

**Keylogger**
Also known as keystroke logging, is a spyware software used to capture which keys are pressed on the keyboard to record text written and passwords.

**Trojan horse**
Is a term used to describe a file that appears to be safe such as Word documents, images or an executable (.exe) you would think is used to install software you like while it also carries malicious code to infect your system and causes damage or enables unauthorised access. Hence, the attacker here injects the malicious code into normal files to deceive you, this is then a form of Social Engineering (refer to the chapter titled ‘Social Engineering – How strong is your human security?’). This attack usually happens when you download software from untrusted sources.

**Rootkit**
A very advanced malware that could give an attacker full control of your device

**Backdoor**
If each web service you use requires an interaction point between your device and the web (a unique door to access you system), a backdoor is an open door in your system that you are unaware of.

**Ransomware**
Malware works by locking access to a device and demands ransom to be paid to the attacker before access to data is restored.

**Scareware**
Malware implementing a social engineering technique to generate money from victims, it usually works by displaying an alert of a superficial malware infection, and then redirects the user to buy a fraudulent removal tool to solve the problem.

**How you can protect your computer**
All computer users can effectively use an anti-virus and other security products to be safe and to keep their devices malware-free. At some point, it was widely shared that the number of computer viruses and malware released for Microsoft Windows is significantly more than those coded to affect

an Apple Mac. The reason arguably being that an attacker plans to affect as many devices as possible while Windows was dominant in the market. Now that Apple has an outstanding market share, more malware continue to be identified for Mac OS X. Recent security reports suggest over a half million infected Macs, that is still less compared to Windows but it really is not only quantity that we should worry about when discussing security. Nevertheless, as an end user, you should consider the condition where a non-Mac malware remains unidentified on your system due to the absence of a malware scanner, it will not affect you but this could be passed through -at some point- to other devices owned by you or someone you know making you an attack vector. The same applies to Linux users such as Fedora, Ubuntu and many others.

Operating systems come with some built-in security, but they still require support by means of third-party products and your safe-use practice as shared below:

- Activate your built-in firewall and other security scanners such as Microsoft Security Essentials at all time before you attempt to surf the web.

Do not attempt to go online without such protection even if it was for a short period of time to update your operating system, it could take few minutes to infect a non-protected computer after it goes online.
- Do not turn off your firewall while connected to a network

Your system has hundreds of doors designed to serve the many applications requiring access to online/network resources. Clearly, it is impossible to monitor all these manually, instead, you need a firewall to close down and monitor these doors and report to you when needed.

It is not enough to have a firewall and an anti-virus, what you are looking for is a security package that should clearly include protection against four main classes of online threat; anti-virus, firewall, an anti-malware (all the types of malware discussed earlier) and finally a protection against Phishing scam (refer to the chapter titled ‘Social Engineering – How strong is your human security?’ for more details on Phishing attacks). Such features are provided by products such as McAfee Total Protection and Kaspersky Internet Security. These are only examples, if you find a solution being offered to you for free from your internet service provider, then go for it as long as it covers these requirements.

- If for any reason you do not want to pay for an internet security package, then at least download a free antivirus and combine it with a free antimalware such as the one from Malwarebytes.

- Not all the features offered by internet security products are useful. You might not need parental control to filter the content of websites you visit, it depends on what you need.

- Create an addition username in your computer that has no system administration privileges (e.g. cannot install software) for your daily use, and for others if the computer is shared.

In addition to these guidelines, go to the end of this chapter and read the device-independent practical security tips you should apply while using the internet.

How you can protect your Apple iPhone and iPad

Apple claims that its operating system (iOS) was designed with security at its core. However, it is important to remember that a technology with no security vulnerabilities does not exist. Risk could come from applications you install or internet connections.

In 2014, many iPhone and iPad security incidents were reported, one of these was caused by a coding error in the implementation of a security protocol, and this has enabled attackers to intercept Wi-Fi communication and read user data in the clear (unencrypted). Same year, a ransomware locked out many iPhone users, additionally, there was the infamous incident of celebrity photos being leaked from the iCloud service which was widely covered by the media.

Nonetheless, you will find no effective mobile security scanners for your iPhone/iPad available from famous firms such as Kaspersky, Norton and McAfee, instead, you will find their security applications are designed to help you locate, backup or restore the data on your device. Apple’s approach is unique as they choose to respond to malware challenges at their end. As such, they ask you to solely install applications from their App Store where they scan all applications code very strictly to identify malicious behaviour before they are made available. That said, new Malware and other forms of attacks continue to occur by exploiting technical and/or human vulnerabilities. This means, under no circumstances should you assume optimal protection. Instead, you should work towards an adequate level of protection by taking security precautions while using your iPhone/iPad as shared below:

- Install your applications from the App Store only.
- Use the ‘Find my iPhone/iPad’ service

It is very useful to locate or remotely lock and wipe a device. Configure these options correctly to use them in case your device is lost or stolen. Also note that similar functionality is maintained by a number of applications from security firms (e.g. McAfee) and is also available in the App Store. You can Enable ‘Find my iPhone/iPad’ from Settings > Privacy > Location Service. You should then open the App Store and install the ‘Find my iPhone/iPad’ application. You can log in from any of your devices to locate the rest.

- Do not rush into connecting your device to a computer or any USB port (e.g. charger) unless you trust the device to be safe. A public computer like the one in your school should not be trusted.
- Make sure the Safari ‘Fraudulent Website Warning’ is set to ‘On’.
- Set an authentication secret from Settings > General > Passcode lock. Make sure you set the ‘Require Passcode’ to ‘Immediately’. It is also possible to use a password (a secret consisting of both digits and letters) by setting ‘Simple Passcode’ to ‘Off’.
- Monitor which websites your Safari browser has stored the password for (if any). This could be done from Settings and Safari > Passwords and Autofill. You can view or delete saved sensitive details such as passwords and credit cards.
- If you want to clear browsing history from Safari in iOS 8, tap Settings > Safari > Clear History and Website Data. For an earlier iOS, tap Clear History > Clear Cookies and Data.
Alternatively, you can also tap Settings > Safari > Advanced > Website Data > Remove All Website Data.

The iCloud is an online cloud computing storage from Apple to store your files remotely and enable access from multiple devices for your convenience. Make sure all your connected devices verify the user (e.g. using passcode) before they can be used, and that your login details for each device is secure.

Nevertheless, do not Jailbreak your iOS device, this will practically destroy Apple’s security model and expose your environment to malicious code. If your device was brand new when you first bought it, and you have not explicitly followed a tutorial or asked someone to Jailbreak your iOS, then you are fine.

In addition to these guidelines, go to the end of this chapter and read the device-independent practical security tips you should apply while using the internet

**How you can protect your Android devices**

Android is by far the world’s most popular system to power smart phones, tablets and many other devices. As an open-source system, there is no restriction on its application development, you can also customise it to have the look-and-feel you want. This marvellous flexibility can be exploited by attackers to infect your system with malware. Hence, just like your computer, look at your Android device as a small computer requiring the support of anti-malware scanners and safe-use practice as shared below.

- Install your applications from known and trusted stores only such as Play Store and Galaxy Apps.

Avoid installing any application from online links using an Android Application Package (APK file), it is very easy for an attacker to add malware to such packages. This also means you must stay away from any pirated apps, not only they are illegal but many (if not most) of these contain malware.

- If you worry your device could be stolen and data on the phone is accessed offline, it is possible to encrypt all your data on both the device and SD card (if you have one). This could be done from Settings > (More) > Security.
- Use the ‘Find My Mobile’ service

Android has an integrated service to locate and lock your device or wipe data remotely. This feature can be extremely important to protect your personal information when the device is lost or stolen. Configure this service from Settings > (More) > Security > Find My Mobile > Remote Controls. Similar functionality is maintained by a number of applications from security firms such as Kaspersky as part of their Internet Security package. In most cases, this service is provided for free.

- Lock your SIM card, set a PIN to protect your SIM card after system restart.
Configure your device to verify and warn each time there is an attempt to install a new application. You can do this from Settings > (More) > Security > Device Administration. At this same location you should make sure there is no tick on the option titled ‘unknown sources’, this will prevent the installation of application from sources other than Play Store.

Get an anti-virus

Most anti-virus apps are available for free. Some users report that certain applications drains their battery, these same security applications worked well on other Android devices. As such, read the reviews relevant to your system and test for yourself which product works best, make sure you get one from a known firm like the ones shared at the end of this chapter. Even if there are attempts to scan application in trusted stored such as the Play Sore, there were incidents were malicious app were removed late, only after thousands of downloads.

Do not ‘root’ your device

By default, your Android system do not share administrative privileges with the user for security reasons, this behaviour protects the system from viruses and malware. However, some advanced users decide to reinstall Android and enable administrative privileges, this makes the device ‘rooted’. The term root is equivalent to ‘Administrator’ in Windows.

In addition to these guidelines, go to the end of this chapter and read the device-independent practical security tips you should apply while using the internet

Further to the guidelines above, what other device-independent security tips should you apply while using the internet?

Keep your system up-to-date

The first advice to start with is to keep your system up-to-date, this is probably one of the most important and effective ways to resist attacks. This includes your operating system (e.g. Windows, OS X, Android, iOS), desktop applications (e.g. MS Office, Browsers) and mobile applications. It is strongly recommended to enable auto-update.

Activate the auto-lock feature in your phone and password-protected screen saver in your computer. Set a reasonable time to lock the screen when the device is left unattended.

A special consideration to keep your security tools (e.g. anti-virus, anti-malware) up-to-date.

Always question the source of any software you install

Read reviews and after you decide that this is a software you need, then make sure you download it from a trusted source. This should ideally be from the vendor directly. While some applications such as Skype, Facebook and Twitter comes from known developers, others are not, try to learn more about the developer of new applications and read the reviews to learn more about its reliability from former users. Then, ask yourself, are there any red flags you can identify in the reviews or description of this product?
You should also revise the list of mobile application you have and remove those you do not use. Question their functionality. If a GPS tracker such as FollowMe and Real-Time GPS Tracker is installed without your knowledge, could it be that someone is tracking your location? Further investigation will be required then to answer this question.

- Always be careful when using web services

Your Operating System including your iPhone/iPad iOS was not natively designed to protect you from web forgery and spoofed web services. Such protection can instead come with the browser you chose to use. Google Chrome and Firefox are good to use. Even if your device is technically secure, many attack utilise forgery and social engineering methods to trick the user, refer to the chapter titled ‘Social Engineering – How strong is your human security?’ and read it carefully.

- Enable GPS when required only.
- Do not install pirated (cracked) software, not only they are illegal but usually come as a Trojan horse carrying malicious code to infect your device and allow unauthorised access.
- Enable authentication secrets (e.g. passwords) whenever offered,

This is usually PIN, text or graphical password, and keep them secret safe. Some new models of mobile devices allow you to authenticate using your finger print, this can be a good option you as it is very hard to guess, impossible to share and takes significantly longer to recover.

- Take backups routinely, if this is difficult, you may want to use a cloud service (e.g. Google account for Android devices) to synchronise your important data.
- If a device is confirmed to have been lost, change the passwords of accounted used on that device immediately.
- Reset and clean up suspicious systems

Reset you device to factory defaults or format the hard drive in the case of a computer when you suspect malicious software has been installed or unusual behaviour regularly recognised or after you buy a used device. Resetting a device should be relatively easy when you have a backup of your contacts and important user data either offline or on the cloud. Formatting a computer is more challenging and could require professional help.

- Avoid connections to Wi-Fi networks in public places such as coffee shops and airports. Alternatively, learn what a VPN service is and use it to secure your own connection in such places.
- Restrict and monitor physical access

Major security concern could remain to be when an attacker has physical access to your device, do not leave your device unattended in when there is a chance it can be stolen.
- Use reputable vendors of internet security products, these include but not limited to F-Secure, Avira, Kaspersky, Avast, AVG, Bitdefender, Intego, Kaspersky, Panda, Sophos, Symantec (Norton) and Malwarebytes.
- If you want to install software or applications for testing purposes, it is good—whenever possible—to try with a device you do not use in your daily life to access work or personal account.
- Do not plug in unknown memory sticks (flash drives), scan them if you have to.
- Do not try to open files on removable media that you do not expect to find.
- Turn off (or hibernate) your computer or at least disconnect it from the internet when not in used for a long time.
- Register your devices

Most devices are supported by their provider, they can be registered with the vendor and you are recommended to take this step. You should also keep an offline copy of the device’s serial number. Additionally, mobile phones can be registered with your network operator, make sure you keep note of the IMEI number of your phone, it is a unique code to identify your device. Identification numbers can also be used to report a stolen device to the police.

Following security guidelines can be time consuming but it is worth the effort on the long run, both: to protect your privacy as well as keeping your device healthy and usable for a longer period of time which saves you money and time.