Queensland Law Society

QLS Guide: iOS (Apple mobile) security for lawyers

A quick reference guide

March 2019

iOS (Apple mobile) Security quick reference

Who should use this guide?

This guide is intended for individual legal practitioners who need to protect their iOS (Apple) mobile devices, or who wish to double check that employer-supplied devices are as secure as they should be.

It is not intended for system administrators or practitioners handling information that might be subject to targeted attack by nation-state actors.[1] Organisations implementing mobile security options should consider the Australian Signals Directorate's *Risk Management of Enterprise Mobility (Including Bring Your Own Device).*[2] Apple also has a very comprehensive security guide available for download here.[3]

For the rest of us, a few basic security measures can mean an iPhone or iPad left in a taxi remains an annoyance rather than a disaster.

Why is this an issue?

Modern phones and tablets hold significant amounts of data and are increasingly used for client work.

There is a persistent myth that Apple devices are not vulnerable to cyber attack. Apple does have security advantages over Android and Windows, but iOS devices are not immune. In 2016 "Pegasus", an iOS specific malware suite enabled interception of email, text messages, secure messaging (including WhatsApp) and files stored on the phone.[4] Criminals follow the money, and the increasing use of Apple products in business is a strong incentive to attack them.

Research conducted by Edith Cowan University's Security Research Institute shows that although nearly all lawyers use their phones for client work (94%), less than half of us (41%) know how to secure them.[5]

A lost mobile or tablet can result in:

- data theft;
- civil liability;
- prosecution by the Legal Services Commission and/or Information Commissioner;
- significant damage to the firm reputation; and/or
- a mandatory data breach notification to all affected clients.

Conversely, simple security precautions may prevent all of these outcomes.

35% of the Australian data breach notifications in 2018 arose from lost and stolen mobiles / data storage devices.

---

[1] This threat is not restricted to classified or defence information. The intelligence services of a number of countries are used to pursue commercial goals or commercial information such as intellectual property or dealings with influential companies in the country of origin. Any solicitor in a larger firm should consider such an attack as a real possibility.

[2] <https://acsc.gov.au/publications/protect/Enterprise_Mobility_BYOD.pdf>.

[3] <https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf>.

[4] Mikey Campbell, *'Pegasus' iOS malware package also found to impact OS X, Apple issues patch* (1 September 2016) apple insider <http://appleinsider.com/articles/16/09/01/pegasus-ios-malware-package-also-found-to-impact-os-x-apple-issues-patch>.

[5] Edith Cowen University, *Client data potentially at risk due to lawyers' lack of cybersecurity* (23 May 2018) Edith Cowen University Western Australia < http://www.ecu.edu.au/news/latest-news/2018/05/client-data-potentially-at-risk-due-to-lawyers-lack-of-cybersecurity>.

If you use an employer supplied or provisioned device

You should

- ensure you are familiar with your firm's mobile technology policy and know how to comply with it:
- periodically[6] ask your firm IT to check that your device remains appropriately protected and walk you through what you need to know to make sure it stays that way;
- consider whether the recommendations in this guide have been applied and, if not, ask what alternative measures to achieve the same objectives are in place;[7] and
- not install new apps or services without IT approval, even if this is not strictly required by your employer's policy.

No solicitor should use a mobile phone without all of these options enabled

Your phone's first and most important line of physical defence is the unlock screen. A pin number or other form of authentication must always be used to lock the phone from intrusion. The phone should lock itself automatically after a defined period of inactivity, and you should think carefully about what can be viewed before the password is entered. To review and change these settings see here.[8]

Generally, older iPhones default to a simple four digit passcode for device access. It is recommended that a pin number be a minimum of six digits, or even better a more secure alphanumeric passcode. To alter this setting on iOS 6 or below see footnote.[9]

A stronger passcode also increases the strength of encryption on stored data, giving added protection from both casual snoops and determined attacks.[10]

Pin, Password or Biometrics?

Short answer: a password is still the most secure, but FaceID or TouchID may suffice.

The technology behind biometric authentication (such as fingerprints, retina scans and facial recognition) is improving, but is not yet foolproof.[11] Another disadvantage of biometrics is that your cooperation is not required – just access to your finger or face.

By way of perspective, most of the hacks to defeat biometric authentication - while not sophisticated - do require a lot of effort (for a description of the steps involved, see here)[12] and law enforcement in many jurisdictions now have powers to compel you to unlock electronic devices whether secured by password or biometrics.

On balance, good passwords are stronger but using one of the more secure biometric options is vastly better than no lock at all. A good security system that you will use is better than the perfect system you don't.

If security over fast access is your preference, a good password or 8 digit + pin number[13] remains the recommended unlock method. Software to unlock phones without the password is readily available,[14] but most of these methods delete the data.

---

[6] We suggest every 12 months, or after major updates.
[7] Solicitors, including firm managers, often (inaccurately) assume that firm IT has implemented a security plan. Unless the provider has been expressly tasked to implement an information security policy they have probably not done so.
[8] <https://www.imore.com/how-to-customize-lock-screen-iphone-and-ipad>.
[9] Steps: iPhone settings → Touch ID & Passcode → Change Passcode → Passcode Options → Custom Alphanumeric Code.

[10] Apple, *iOS Security Guide – White Paper: January 2018* (2018) 15.
[11]<https://this.deakin.edu.au/innovation/facial-recognition-id-how-safe-is-your-face>.
[12]<https://thehackernews.com/2017/11/iphone-face-id-unlock-hack.html>, but this is not easy – see <https://www.wired.com/story/tried-to-beat-face-id-and-failed-so-far/>.
[13] A password of the same length will be more secure than a PIN as there are a lot more available characters.
[14] https://www.imyfone.com/ios-data-erase/how-to-unlock-iphone-without-passcode/>.

Ensure the “find my iPhone” feature is on (and “send last location”, which sends a map location just before the phone battery runs out – iOS 8 and above.) See support guide here.[15]

This enables a lost/stolen phone to be traced or wiped. This feature cannot be turned on remotely after the event, so make sure it is done beforehand.

Even if “find my iPhone” is not enabled you can reset the passwords to all online services, but this will not erase the data already on the phone.

A good password and ability to remotely erase data may avoid the necessity of a mandatory data breach notification if the device is lost.

Security Updates

It is important to ensure that your phone is up to date. Most malware exploits known vulnerabilities and these are patched fairly quickly by vendors. Only devices which are not kept updated will remain vulnerable to these attacks.

Apple – as a unified operating system – has an advantage in the rate of upgrades and applying these promptly can add to your security significantly. Security patches and minor upgrades should be set to run automatically. For instructions, see here (Mac) or here (iPhone/iPad).

Upgrading the iOS version may need some thought as well as extra space. Once you decide to upgrade it is easy, see here.[16]

Extra Protection

An antivirus/antimalware product from a reputable source can be a good additional layer of protection for an Apple mac or iPad, although whether they are of any real benefit on iPhones is controversial. The most tangible benefit of third party security software for iPhones is probably to identify Phishing links and malicious websites (see below).

Having said this, malware directed at iOS used to be rare, but it is increasing rapidly.[17]

Don’t use a “jailbroken” phone

Jailbreaking a phone (altering the operating system software) bypasses important security features. Such a device should not be used for business purposes unless it has been configured by an expert.

There is no simple test for jailbreaking but there are some symptoms that can be checked.[18] Unless there is a good reason that your phone is Jailbroken it can indicate that someone has installed attack software on it, so think before restoring it as you may delete important evidence of this intrusion.

Jailbreaking is not the same as unlocking the phone from a carrier network.

Be very cautious about installing apps

Malicious apps can do anything from harvesting passwords to spreading malware.

Apple tests and verifies apps, but does not warrant that they are free from hostile intent. The checking process does not prevent an app asking for inappropriate levels of data access and there are no controls on what happens to the data once it is uploaded to the app vendor.

As a rule of thumb, the fewer apps on a device the more secure it will be.

---

[15] <https://support.apple.com/en-au/HT201472>: To check if Find My iPhone is enabled in iOS 6, 7, open Settings, tap your name at the top of the screen, and then tap iCloud > Find My iPhone.

[16] <https://support.apple.com/en-au/HT204204>.

[17] <https://blog.malwarebytes.com/101/2018/03/the-state-of-mac-malware/>.

[18] <https://www.certosoftware.com/detecting-iphone-spyware-guide/> (Note, QLS is not advocating you buy this software, but the checklist is useful).

General tips for mobile computing

Passwords and authentication

One of the best protections for online data is to turn on two factor authentication. This should be applied to all iTunes/Apple ID, Office 365, password manager, Authenticator app, internet banking (mandatory for Trust Accounts)[19] and any email account that can access (or reset access to) confidential client data.

Two factor authentication is a system that requires anyone seeking to access an account to supply not only the password but another means of authorisation, such as a fingerprint or one time code supplied via SMS or an authenticator app. The authenticator app is the more secure option.

If an attacker obtains your password (through phishing or some other method) they will not be able to log into the account without supplying the additional code. This can be set up in different ways – either requiring the code every time you log on, or perhaps more periodically.

An excellent resource for implementing two factor authentication on many online accounts is available here. An Apple specific source can be found: here.

Use good passwords. Don't re-use passwords. If following good password security drives you nuts (as it does most people), use a password manager. See QLS resource here.

Don't use free wifi

An attacker can use a simple wifi device to steal passwords and information from a phone, tablet or laptop connecting to the network. These attack devices are small, cheap and can be easily planted in public spaces. The attacker can broadcast any wifi name they choose, simulating the legitimate networks of hotels, cafes and public places.

Even legitimate wifi equipment might be infected with malware, potentially compromising your phone. If you must use free wifi, a VPN service can reduce but not eliminate some of the risks.

Website Access

Before accessing a website, check the URL (site address). URL's beginning with 'https' are secure communication computer networks, while URL's beginning with 'http' are not.[20]

"Https" does NOT mean the website is "safe" or that it is not malicious. All it means is that communication with it is less likely to be intercepted by a third party.

The limited screen space on a phone makes checking URL's and links harder. Web browser extensions are available that automatically check this for you.

Phishing

Because iPhones are harder to hack, the most common successful attack against an Apple user is a phishing attack. In fact, an iPhone user is 18x more likely to fall victim to Phishing than malware.

Phishing is the use of fake messages to get you to download malware or insert your password into a fake website. Because of the smaller screen and on-the-go immediacy of remote working, we are three times more likely to fall victim to phishing on a mobile than a fixed computer.

The starting point of most phishing attacks is getting the target to follow a link. Links in SMS, email, apps or websites can be used to trick users into visiting a malicious page, or downloading an infected app or file.

The best way to avoid infection is to not visit any links that you don't trust, especially from unknown sources, such as via SMS. Unfortunately, a trusted source is not a complete protection. If someone

---

[19] See the QLS Costs Guide.
[20] Philippe Doyle Gray, 'The pillars of digital security' [2014] Summer *The Journal of the New South Wales Bar Association* 46, 58.

else's device is already infected, messages from their account can be loaded with content devised to infect or hijack you as well.

Never insert your email or other password to access a message or attachment. If you are being prompted to re-authenticate to use a service, go to the website or app and do it there, and do not use any links received by SMS or email.

For more information about phishing generally – see here.

Other social engineering attacks

An email from your boss or client asking you to do something may not be from them. If their email has been compromised or "spoofed" you may be dealing with an attacker. Away from the office and distracted by other tasks, a mobile user is more likely to fall victim to this kind of social engineering attack.

Do not transfer funds, open links or forward sensitive information on the strength of an unverified email request.

Enquiries: David Bowles
Direct line: 3842 5937

Lead Authors: David Bowles, Ethics Solicitor
Liam O'Shaughnessy, Ethics Clerk

CHECKLIST – iOS Security (Individual users)

	What?	Why?	How?
☐	Unlock password: minimum of 6 number pin (8 numbers better), password or FaceID.	Protects against physical intrusion if device lost or tampered with.	
☐	Screen locks automatically. Sensitive data not viewable before screen unlocked.	If a phone is unlocked when it is stolen the data on it is insecure. Information visible from the lock screen is also insecure.	Lock screen options: here
☐	"Find my iPhone" and remote wipe features turned **on**.	Allows recovery of a lost device or erasure of data if connected to a network. Must be turned on before device lost/stolen.	Find my phone guide: here
	Ensure the device is running the most up to date apps and operating system.	Most malware attacks exploit vulnerabilities that have already been identified and fixed. Only devices that are not kept up to date will remain vulnerable to the majority of viruses and other malware.	here (Mac) or here (iPhone/iPad)