Queensland Law Society®

QLS Guide: Android security for lawyers

A quick reference guide

March 2019

Android Security quick reference

Who should use this guide?

This guide is intended for individual legal practitioners who need to protect their 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]

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

Why is this an issue?

Modern phones are essentially laptops that fit in your pocket. They contain significant amounts of data and are increasingly used for client work.

Research conducted by Edith Cowan University's Security Research Institute shows that 94% of lawyers use their phones to hold and process confidential client data, yet less than half of that number (41%) know what basic security measures are enabled.[3]

Without that understanding, solicitors may fail to use appropriate safeguards or inadvertently turn off security measures. Those of us using our own devices may have no protection enabled at all.

An unprotected mobile or tablet can lead to data theft, civil liability, prosecution by the Legal Services Commission and / or significant damage to the firm reputation arising from a mandatory data breach notification. Conversely, simple security precautions may prevent all of these outcomes.

35% of the notifications under the Australian mandatory data breach regime in 2918 arose from lost and stolen mobiles/data storage devices.

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[4] 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;[5] and
- not install new apps or services without IT approval, even if this is not strictly required by your employer's policy.

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

[4] We suggest every six months, or after major updates.

[5] Solicitors, including firm managers, often make unfounded assumptions about the scope of responsibility of firm IT suppliers for information security. Unless the provider has been expressly tasked to implement an information security policy they may not have done so.

First layer security: No solicitor should use a mobile phone without all of these options enabled

The main protection is your phone unlock screen. A pin number or other form of authentication must always be used to lock the phone from intrusion by third parties. The phone should lock itself automatically after a defined period of inactivity (these controls are all found in “lock screen” settings).

Pin, Password or Biometrics?

Short answer: A password is still the most secure, but fingerprint or swipe may suffice.

The technology behind biometric authentication (such as fingerprints, retina scans and facial recognition) is improving, but is not yet foolproof. Each of those methods has been defeated using relatively simple methods. Fingerprint and retina scanning are the hardest to fool, voice and face recognition the easiest.

By way of perspective, most of the hacks to defeat biometric authentication - while not sophisticated - do require a lot of effort (If you are curious, see hacks for: facial recognition[6] retina scanning[7] fingerprints). 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.[8]

If security over fast access is your preference, a good password or 8 digit + pin number[9] remains the recommended unlock method. If you need faster access, a swipe pattern that uses at least 6 of the available points and does not rely on a simple shape may be a good choice, or use the fingerprint scanner. Especially if you have your most confidential data behind a second layer of protection, swipe or biometric access on the latest phones should be enough to stop casual intrusion.

Changes to lock method can be accessed in [settings/lock screen and security/secure lock settings]

Add your Google account to the phone, and ensure the “find my phone” feature is on. (See support guide here)[10] This provides the ability to find, lock or wipe a lost device, albeit at the price of reduced personal privacy. Turning off location settings disables this function.

Newer phones (Android 7.0 and above) encrypt internal data by default, but older systems (Android 5.0 – 6.0) may need this activated.

“External” data (stored on the SD card) is usually not encrypted by default. Turn SD card encryption in [Settings/Lock screen and security/Encrypt SD card]. This prevents files being accessed by removing the SD card and inserting it into another device. However, it also prevents you accessing contents if the phone is damaged, so make sure important files are backed up.

These three settings alone may avoid the necessity of a mandatory data breach notification if the device is lost.

Second layer security

It is good practice to place your critical data, authentication apps, banking and client confidential email behind a second layer of encryption and security.

The basic version of this system is an app lock which requires a second password to unlock specific apps. This enables you to use one of the quicker access methods on the lock screen but still have a higher overall security for more confidential information on the phone. Reputable brands such as Norton supply app lock apps, available through the Play Store.

The full (and far more effective) version is a “sandbox” which permits you to set up a “phone within a phone”. This partitioned area is not only guarded by an additional layer of passwords/biometric

[6] <https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/#66888cb61330>.
[7] <https://arstechnica.com/information-technology/2017/05/breaking-the-iris-scanner-locking-samsungs-galaxy-s8-is-laughably-easy/>.
[8] As at February 2019 fingerprint locks are the best trade off between ease of use and security. Retina scanning is secure, but often does not work well under different lighting conditions.
[9] A password of the same length will be more secure than a PIN as there are a lot more available characters.
[10] <https://support.google.com/pixelphone/answer/3265955>.

authentication but contains a second set of apps which are electronically quarantined within a protected zone. In theory, data in the sandbox is protected from intrusive apps or viruses on the main part of the phone.[11]

An example of this kind of system is “Work Profile”/“Android for work”, which is an enterprise grade system that allows an employer to set up and remotely manage a protected zone on an employee’s phone. Only work approved apps can be installed in the protected area, and many of these can be controlled by the employer. Setting this up is complex and must be integrated into a wider management system.

Samsung Knox (now called Secure Folder) is similar, and can be used on Samsung phones without your employer having the enterprise management system at their end. A quarantined folder is set up with protected apps installed within that separate environment. To implement Secure Folder see here.

For non Samsung devices an app called “Island” from the Play Store can achieve a similar outcome. However, the developers have the rather alarming warning on their website that the app is in Beta version and “may brick (ie, render un-usable) some devices.”

Extra Protection

An antivirus / antimalware product from a reputable source can be a good additional layer of protection. For a comparison table (2019) see here. Some argue that anti-malware is not essential for phones. In our view, the significant consequences of a data breach on a solicitor’s phone substantially outweigh the cost of purchase and slight impact on performance of running an anti-malware service.

Security Updates

It is important to ensure that your phone is up to date with the most recent security updates,[12] and, if the device is too old to accommodate the most recent updates, that you consider purchasing a new one.[13]

Some of the newer Android phones receive monthly security updates. To check when the last security update was released, open your phone’s settings, scroll to the bottom and touch ‘About phone’ and then ‘Android security patch level’. The date displayed will be when the last security update was released. [14]

Don’t use a “rooted” phone

Most phone suppliers lock users from the base (or “root”) layer of the operating system. This can be annoying, permitting the supplier to force apps and other settings that tie up resources and slow down your phone. Removing these restrictions is called “rooting”, and there are numerous instructions for doing this on the internet.

However, a Rooted phone may no longer upgrade automatically, and is far more vulnerable to malicious apps. Do not use such a device for business purposes unless you are an expert.

Be very cautious about installing apps

Malicious apps can do anything from harvesting passwords and confidential information to inserting malware into outgoing messages.

Apps in the Google Play Store have all been verified and must comply with basic security guidelines. Apps downloaded from other Stores may not get the same (or any) scrutiny and should be avoided. Google Play Protect is enabled by default on Android 7 phones onwards. The built-in malware protection checks the device and apps on it every day and removes anything malicious.[15] To make sure it is still turned on:

[11] It is not possible to claim this definitively as it depends upon how your apps handle data.
[12] Android, above n 4.
[13] Handmer, above n 2, 68
[14] Android, above n 4.
[15] Android, above n 4.

1. Open your Android device's **Google Play** Store app.
2. Tap Menu (top left, three horizontal bars) then choose **Play Protect**.
3. Make sure Scan device for security threats is: **ON**.

Even “official” Play Store apps must be treated with caution, as malware can be introduced with updates, and many apps allow very high levels of access to data. The verification process is not invulnerable and in 2018, several fake bank apps stayed undetected in the Play Store for months.

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

To avoid accidentally installing unapproved apps, for older versions of Android - Open Settings/Security and check that the box “Unknown Sources” is **NOT** checked. Newer versions have this turned off by default.

General tips for mobile computing and data access

Passwords and authentication

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.

One of the best protections for online data is to turn on two factor authentication. This should be applied to your Google account, Office 365, password manager, Authenticator app, internet banking (mandatory for Trust Accounts)[16] and any email account that can access (or reset access to) confidential client data.[17]

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 (These apps are free – Google Authenticator or Microsoft Authenticator, for example). Next level up is a security key, such as a YubiKey or Titan key.

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.

Don’t use free wifi

An attacker can use a simple wifi device to steal passwords and information from any 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.

[16] See the QLS Costs Guide.

[17] Handmer, above n 2.

Look at the first letters in a web address: Https vs Http

URL’s beginning with ‘https’ are secure communication computer networks, while URL’s beginning with ‘http’ are not.[18]

“Https” does NOT mean the website is “safe” or 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,[19] or alternatively, by using the Safe Browsing protection in Google chrome, you will be warned and taken back to safety should you stumble upon a malicious site.[20]

Phishing

Phishing is the use of fake messages to get you to download malware or insert your password into a fake website. Phones are now a primary target for phishing attacks.

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 final stage of a cyber attack is often to use the target system to spread malware, so even if you know the sender you cannot be sure that the message is safe.

The best way to avoid infection is to not visit any links that you don’t trust and to check the end destination for any link carefully. Google does have inbuilt ‘safe browsing’ in apps such as Chrome and Gmail, which can help provide protection, but are not foolproof.[21]

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.

If you must follow links – be very careful

Often the URL for the fake website will be almost – but not quite – exactly the same as the legitimate site’s – a .biz rather than a .com, for example. Some foreign languages display differently on handsets, allowing an attacker to present a URL that is visually identical but electronically very different.

Enquiries: David Bowles
Direct line: 3842 5937

Guide co-written by Liam O'Shaughnessy, Ethics Clerk

[18] For a full explanation see: Philippe Doyle Gray, ‘The pillars of digital security’ [2014] Summer *The Journal of the New South Wales Bar Association* 46, 58.
[19] Ibid: The article recommends the use of ‘HTTPS Everywhere’ published by the Electronic Frontier Foundation.
[20] Android, above n 4.
[21] Ibid.