Personal Comms Security

Are you smarter than a seven year old? Just recently during a monitored ethical hacking demo in England, after watching a demo on You Tube a seven year old hacked into a shopping centre Wi-Fi network. In less than 11 minutes, she was able to access, watch and intercept data from devices using the network. Potentially, she could have used the information gathered for illegal purposes[1]; however, the demonstration was deliberately set up to test the robustness of the system and show just how vulnerable our information is. Despite technology becoming more complex, breaking into it can be child's play.[2]

This article will provide hints and tips on some basic security measures which will help you use personal IT devices securely and safely. It is the first of a series of articles inspired by our use of social media and was collated from open source materials. There are many more tips and useful websites out there, so if you have any you want to share, email CAL.Lessons@defence.gov.au.

Technology is an integral part of our lives. It is used to stay connected to friends and family, manage personal admin, such as bank accounts, and improve productivity and connectivity at work. It is wise to consider how we can protect ourselves, our information and our workplace. Whilst it is easy to become a bit paranoid about the threats, it's important to remember that most risks are readily managed by employing a few basic security principles and being smart about how, when and where you use your device. To combat the threats you need to:

- be informed, by understanding the threat environment
- apply the basic security principles
- follow sensible security practices

The following hints and tips will provide you with the tools to address these threats.

Tip 1: Be aware of the threat environment

It is important to be aware of the threats that exist and then know how to protect your device from them. Our mobile devices provide us with the ability to manage our lives whenever and wherever we like. We are free from the constraints of the desktop or even laptop, but with that freedom comes responsibility. Opportunities can quickly become threats if not managed properly. For example, on desktops we use passwords and anti-virus software as an everyday part of smart IT practice, but both are still employed in limited ways on mobile devices.

Our mobile devices face the same level of threat, if not more, than those faced in the desktop environment. If you think of your phone as a mobile mini-computer, containing your entire address book, social media profile and important personal data, then the concepts behind securing your privacy, identity and information becomes clearer.

---

[1] **WARNING!** Do not try this for yourself. It is highly illegal.

[2] Source : http://www.dailymail.co.uk/sciencetech/article-2919762/Hacking-Wi-Fi-s-child-s-play-Seven-year-old-shows-easy-break-public-network-11-minutes.html

Threats to your device include (but are not limited to):

- **Device loss or theft.** Software and cables exist that are able to circumnavigate security measures to strip your data and images. This can result in the loss of sensitive personal information, which can expose you to identity theft or compromise your online accounts. Losing a device may also mean not only having to pay for a new one, but potentially paying for any calls, texts or data usage charged to your account.
- **Phishing and other scams**. These will often appear as unsolicited or unusual emails from contacts, texts or on social networking sites. These scams are designed to procure sensitive information such as account numbers and login credentials often without your knowledge. As a result, unauthorised withdrawals could be made from your bank account.
- **Malware and Spyware**. These programs will not only track your metadata, site usage and lifestyle preferences, but also have the potential to compromise more sensitive information. They enable identity theft, unauthorised usage of your mobile phone and provide the ability for someone to listen in on your phone calls and retrieve your voicemail.
- **Quick Response (QR) codes**. QR codes are used for a variety of purposes, and make the sharing of information, particularly for marketers, very easy. Scanning the QR code allows you to display text, contact information, connect to a wireless network or open a web page in your device's browser. They allow you to store bank account details and your résumé, access virtual stores or automatically connect to your PC. You can also accidently download a malicious application via a QR code, compromising your personal security and the functionality of your device.
- **Wi-Fi networks**. These networks are becoming more widespread. There is no doubt they are useful but unfortunately they are not completely safe. Even when connecting to a secure network, you run the risk of having sensitive information such as passwords and account numbers intercepted and used without your knowledge.
- **Apps**. There are many apps that actively mine your personal information to sell to third parties. Some even turn on your GPS without your explicit knowledge or permission.
- **Jail breaking**. Some people hack their own device to bypass security measures so they can download more apps. This will cause problems as it can expose a device to additional threats.
- **SMS Hacking.** SMS is among the top ways for hackers to break into mobile devices and steal information. The hackers achieve that by fooling mobile users into clicking on malicious links in a fashion similar to phishing in email.
- **Token security efforts.** One recent report found that the majority of users still access their PC or devices using a password such as "password", "123456" or a simple variation.[3] It's time to get serious about security. Good security underpins successful and safe online experiences and interactions.
- **Keystroke Logging –** Keystroke logging refers to the action of recording the keys struck on a keyboard. There are several key logging methods from software based, where programs monitor each keystroke, to hardware based,

[3] Source: https://www.teamsid.com/worst-passwords-2015/ Note that Splash Data obtains this information from researching over 2 million leaked passwords. It's that easy!

where either the keyboard itself, or another device is added to monitor strokes. This may give people access to your user names and passwords for many of your accounts. Avoid using public or unknown computers to access sensitive information, and implement the use of anti-spyware/anti-virus programs, as many of these are able to detect software based keyloggers.

Tip 2: Become tech savvy and stay informed and up to date with the latest information on security threats and countermeasures - knowledge is power.

It's easier than you think to become tech savvy. Get to know your PC and/or device, so that you understand where all of the settings are and what they do.

- Familiarise yourself with basic jargon so that you know how best to apply the most robust security settings you can.
- Read manufacturer's advice on the best security practices that you can apply to your particular device. General hints and tips will provide you with basic security coverage, but you will need to be fully conversant with the requirements associated with your device brand and model.
- Some devices are safer than others. Understand the capability of your device and take any additional measures you can to improve its security.
- Know what you are doing to your phone when you are playing with the settings. Conduct frequent checks to see if downloaded apps have automatically changed your settings without you realising it.
- Note that currently, hackers prefer to target Android platforms.

There are many websites that can provide you with the latest information on internet security threats. They can also provide you with practical tips and hints for staying safe on line. Some of these include:

- Defence Security and Vetting Service
- Defence Signals Directorate
- Department of Communications and the Arts, which has links to Stay Smart Online (which also provides a safety alert service)
- Office of the Children's eSafety Commissioner (with links to the Cybersafety Help Button)
- Australian Cybercrime Online Reporting Network
- Australian Communications and Media Authority
- The Office of the Privacy Commissioner
- Whirlpool.net.au
- Snopes.com
- SANS.edu will provide you with a comprehensive understanding about the dangers of default passwords
- privacygrade.org will provide you with information on App safety
- your ISP, anti-virus software company or device manufacturer websites provide frequent updates and information on security matters
- Chief Information Officer Group

Tip 3: Employ basic security principles

There are a number of measures that you can take to ensure your security. Basic security principles that are applicable to all mobile devices and will effectively counteract most threats include:

- Keep your device closed. Never leave it unattended in public. Consider keeping location settings enabled and using the Find my iPhone app to enable you to get your handset back if you lose it.
- Every phone has a unique identification number (IMEI). Find out what yours is by dialling *#06# (star, hash, zero, six, hash) then write it down. Knowing this will help your service provider block your phone from being used if it is stolen.
- Update your software. Install the latest available version of the operating system.
- Install antivirus software. Check out the different companies' websites to be informed about what you use.
- Secure lock your screen by using a pin or password to gain access to your PC/ device. Secure your password and keep it to yourself. Make sure that you use complex arrangements of letters, numbers and symbols. Configure your device to automatically lock after a certain period of time.
- Consider using a SIM lock. This requires you to put in a PIN to make a call or send a message. It's a valuable tool if you are on an uncapped contract and misplace your phone.
- Don't hack your own device! Don't jailbreak your iPhone or root your android system. It breaks down your operating system and makes it easier for malicious codes to access your details.
- Turn off the GPS when not using it. Your pictures can be geotagged, enabling unwanted viewing of your images by strangers.
- Only shop at reputable app stores. If using android deselect the "unknown sources" option in your device's applications settings menu. Remember that a seemingly "free" app may be employing other means to generate revenue. Unscrupulous providers will do this by capturing data and connecting to other services that charge to your account.
- Dispose of your device in accordance with the manufacturer's recommendations. Use the code provided to erase or overwrite stored data.

Tip 4: Use best security practices to safeguard your information

Safeguard your information by applying the following principles:

- Confine your profile access to a limited number of devices.
- Enable secure browsing so that you only view your profile on https: secure application protocol. Double check the URL when sending sensitive information. Consider using your bank's official app so that you know that you are going to the right place every time.
- Use different passwords for different accounts and functions. Use passwords that combine a series of words, utilising a series of upper and lower case letters as well as other characters. Such as "Th3GoldenM0nkeY", as passwords like these are very unlikely to be in dictionaries that an attacker could use. Passwords longer in length are also considerably harder to crack, aiming for 15+ characters is good

practice. Consider using a password management app to keep all of your passwords in a secure vault behind a single strong password. Password generators are also useful. Remember, the easiest passwords to remember are the easiest ones to hack. Android face locks are also not effective. Make sure that any boxes that say “make passwords visible” are unchecked.

- Change your password frequently. In public, it is easy for someone to watch what you are typing.
- Don’t store your passwords on your device.
- If your browser ever warns you that a sites certificate has a problem or is not trusted, do not proceed to that site and don’t visit it again.
- Know your apps and their privacy conditions. Many apps, masking themselves as entertainment or even as useful, actively mine and strip your information and data. Dangerous apps can be as diverse as GO Locker, Camera 360 Ultimate and Words With Friends. Some apps such as Tinder automatically turn on your GPS. Before you sign up for an app, consider what it is asking you for permission to access and why. Check out other users’ reviews and ratings. There are a number of sites that provide app safety advice. Check out http://privacygrade.org/ and take it from there.
- Delete unnecessary or sensitive information, such as SMS with bank details. You can encrypt SD cards, but it is better to make sure that sensitive information is not kept on your phone in the first place. Some devices support the utilisation of external usb drives.
- Back up your data. This will enable you to restore the information on your device if it is lost or the information is deleted.
- Avoid texting or emailing personal information. Even if you receive what appears to be an official request, only respond by contacting your bank or the requesting organisation personally to confirm the request.
- Think before you click on links, MMS or attachments in unsolicited emails or text messages. If one of your contacts has had their profile hacked, automatic emails may be sent from their address. Additionally, scam emails can look like they came from a contact, but when you hover over the sender the real source email address is revealed. If it looks dodgy, then it probably is. Delete it and discuss it with your contact so that they can secure their profile again.
- Consider using kid/guest modes. This protects your information from inadvertent access to or using important information (like phoning your boss) by unknowing family members.
- Log out of sites instead of just closing the browser. This is particularly important if using public computers. Delete the browsing history as well, just to make sure.
- Bluetooth creates a window through which someone can hack into your phone. Turn it off when not in use. Turning off your Wi-Fi when not in use is also an essential security measure. Make sure you disable any automatic connections to Wi-Fi. Turning them off saves battery power as well!
- Only use secure wireless services. Public Wi-Fi is convenient and is useful when your allocation is running low, but it involves compromising your security.
- Avoid accessing and using social media, online shopping or banking, sending confidential emails, entering passwords or credit card details, online documents or forms on public Wi-Fi systems.
- If you have to do any of the above, always use encrypted (password protected) networks. Choose networks with WPA2 and WPA encryption for the highest level

of security. Look for the https: application protocol or the lock symbol when accessing the network. Select a public identity or try to use a Virtual Private Network (VPN) as they encrypt connections at the sending and receiving ends.

- Always ensure that you are updating and patching your trusted applications and operating system. This will repair threat vectors that have been identified by the publishers to provide a more secure product. This also sets back individuals who have also identified these gaps and may have attempted to exploit it.

Part of your routine

Just as using a device has become integral and essential to our everyday lives, using security measures to protect yourself and your information is also essential. Making it part of your routine will not only help you manage your personal security, but also ensure that your online profile is secure.

The next article on this topic will provide information on content with a special focus on social media. It is aimed to coincide with the release of the Chief of Army's latest Social Media Directive.