March 2017

Top Security Tips for Personal Device Use

Introduction

1. There are a lot of things to think about when it comes to the security of personal devices (e.g. smartphones, tablets and laptops) and the information they store. Compromises of personal devices can have significant productivity, financial and emotional impacts.
2. This document has been written to assist with identifying the top security tips to secure personal devices and protect your information.

Top security tips

Use legitimate software and keep it up to date

3. It is important that personal devices are configured to automatically apply updates as updates for applications and operating systems are regularly released by vendors to resolve security problems. Further, new versions of applications and operating systems regularly include additional security features to make it more difficult for personal devices to be compromised.
4. When operating systems on personal devices are not supported by vendors you will no longer be able to receive updates, and consideration should be made to change to a device which is currently supported. For example, many Android-based smartphones are not supported and will never receive updates.
5. When purchasing new personal devices, consideration should be made to select a device that is currently supported by a vendor that has a proven track record of providing timely updates. For example, while all new Apple iPhones will be supported with updates, only premium Android-based smartphones will be supported with updates, albeit to varying degrees depending on the particular vendor.
6. Finally, you should always use legitimate applications that you have purchased from a physical store, a trusted app store or downloaded from a reputable vendor's website. If you use pirated applications, or untrusted app stores, personal devices may become compromised or won't be supported by the vendor with updates. Additionally, care should be taken to avoid applications that ask for excessive or suspicious permissions.

Back up your important files

7. Save all your important files onto a USB stick, memory card, external hard drive or online storage service. Ensure USB sticks, memory cards and external hard drives are not left connected to personal devices after your important files have been backed up.

8. If you have a problem with personal devices and they need to be reset or replaced, you will still have access to your important files if you have completed recent backups. Likewise, if personal devices are compromised by malicious software that prevents you accessing your important files until you pay a ransom, having recent backups can assist you in recovering your files.

Prepare for lost or stolen personal devices

9. One of the biggest risks to your information is from lost or stolen personal devices. Know where personal devices are at all times, avoid leaving them unattended when away from your home and if leaving them at home store them in a secure location. If personal devices support a 'find my device' function or the ability to encrypt your device these measures can provide additional security in the event of it being lost or stolen.

Be suspicious of unsolicited phone calls, SMS, instant messages and emails

10. Unsolicited phone calls, SMS, instant messages and emails are trying to get you to do something that will benefit someone else. It might just be spam trying to get you to buy things or it might be trying to get you to access a file that will compromise your personal device; access your information (such as your online banking details); or to produce revenue for someone else via the use of premium phone numbers, advertisements or app downloads.

11. Do not follow instructions from someone who rings to tell you your personal device has technical problems. Further, if someone has sent you an SMS, instant message or email that you think is strange (including requests to click on a link, open attachments or to provide a password) delete it.

Use anti-virus software

12. Use anti-virus software from a reputable vendor for personal devices and keep it up-to-date with an active subscription. Anti-virus software does not have to be expensive. Some operating systems even come with free anti-virus software built-in.

13. Anti-virus vendors ensure their software helps prevent personal devices from being compromised. If you have a current and up-to-date version, you can be assured that the software is looking out for problems and stopping them where possible.

Use a screen lock

14. A screen lock with a strong password that contains a combination of upper and lower case letters, numbers, and symbols where possible, should be used for personal devices. Swipe or gesture-based passwords can be easy to guess and should not be used.

15. If personal devices support biometric identification (such as a fingerprint scan) this can provide a convenient way to unlock a device after a password has initially been used to unlock the device.

Use different passwords for different websites

16. Use different passwords for different websites, especially for any websites that store your credit card details or any other sensitive information. If you use the same username (such as an email

address) and password for a number of websites, and one website is compromised, someone accessing that information is more likely to be able to access other websites which you commonly use.

17. Some websites offer the ability to use multiple steps to logon, such as a number sent via SMS to your mobile phone in addition to you using your username and password. The use of such mechanisms, even though they may be slightly inconvenient to use, offer far greater security and protection for your information.

18. It is also important that any email address you use for password recovery for websites has a unique password. Someone that knows the password for such an email address could use the 'password reset' functionality on websites and use the reset email that is generated to gain access to that website even if they didn't originally know the password for that website.

19. Finally, don't use 'remember my password' functionality within your web browser. This can place your passwords at an unnecessary risk of being compromised. If you struggle to remember passwords, consider using a trusted password manager application or writing them down and storing them securely and separately to your personal devices.

Avoid free wireless networks

20. Whilst the use of free wireless access may be alluring, their use with personal devices can often put your information at risk. Free wireless by its very nature is unsecure, this can expose your web browsing sessions to someone looking to monitor your activities. Where possible use internet access from your telecommunications provider, or if the use of free wireless is unavoidable, avoid undertaking any sensitive activities.

Monitor your online presence

21. Check your privacy settings on social media platforms to make sure you know who can see your information. Privacy settings sometimes change after functionality is added to social media platforms so it is important to check them regularly.

22. It is best not to put personal details online. Also, consider checking the information that others put online about you. While some information might not seem important, many pieces of information can be put together to form a picture about you. Never assume that anything you do or post online will remain secret.

23. Many high profile websites have been compromised resulting in the release of highly sensitive information about their users. If your personal information is accessible online it can be used against you. This could range from something as simple as sending you spam emails to something as serious as accessing your accounts and stealing or deleting all your information, or even identity theft.

Contact details

24. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

25. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.