TOP TIPS

SAFEGUARD YOUR DEVICE

IT'S HOW WE CONNECT

Digital devices now play a central role in our (online) lives, so it's worth taking a few precautions to keep them safe.

1. INSTALL SECURITY SOFTWARE OR ACTIVATE NETWORK-BASED PROTECTION

Installing security software (often referred to as 'anti-virus' software) on your computer will help manage many online threats. Security software packages typically include groups of features such as anti-virus, anti-spam and firewalls. Security apps (applications) are also available which can help identify many risks that affect mobile devices. Ensuring your security software is up-to-date is essential as this will help protect against the latest threats.

Many homes now have internet TVs, game consoles, set-top boxes and Wi-Fi-connected tablets and mobiles that can leave your family susceptible to scams, fraud and inappropriate content. If your service provider offers it, then choose home broadband and mobile services with network-based protection and parental controls to help protect all devices. We recommend Telstra Broadband Protect and Telstra Mobile Protect.

2. REGULARLY UPDATE YOUR OPERATING SYSTEM AND APPLICATIONS

Out-of-date software can mean your device is vulnerable to known attack techniques. Hackers and cyber criminals commonly target vulnerabilities in old versions of software that have not been updated by a user. Check regularly for updates to your operating system, and also for each app you use. Many can be set to automatically update in their settings. Examples of common mobile operating systems include Android and iOS; and common computer operating systems include Windows and OS X.

3. SET A PASSCODE-PROTECTED LOCK-SCREEN ON YOUR DEVICE

Set a passcode/password on your device so the screen locks while it's idle (switched on but not in use). Also set your device to automatically lock after a few minutes. It might seem trivial, but if you leave your device behind or it's stolen, you want to be confident your device is locked. Go to your device's settings to choose a passcode lock with auto-locking.

4. BE AWARE OF WHERE YOU GO ONLINE

Pay attention to the website address (URL) at the top of your internet browser when you're online. Clicking a link can send you to another site. Viruses and other malicious users can try to access your information on your device when you click a bad link, open a bad file or even just by visiting a dodgy site. If you're uncertain or suspicious, use your judgement, play it safe and leave.

5. BACK UP IMPORTANT DATA REGULARLY

'Backing up' means making a copy of your information and storing it safely on a separate system, often in a separate location. Whatever goes wrong – fire, theft, failure, disaster, carelessness or a virus – a back-up copy of your data ensures your important information is safe. It can be used to restore missing data back to a device. It is also a good idea to be familiar with your devices inbuilt services that help to locate or wipe (erase all data) should you ever lose your device.

6. FINISHED WITH YOUR OLD DEVICE? WIPE IT CLEAN

Before you forget about your old device, recycle it or pass it on to someone else, it needs to be cleaned of all your data and settings. The next user should not be able to access any of your information, including images, files, emails or videos. Go to your device's settings and choose to 'Erase all contents and settings', 'Factory data reset' or similar.

After you have erased the data from your device, consider recycling it and the accessories for free with MobileMuster, mobilemuster.com.au.

Visit recyclingnearyou.com.au to find out where to recycle your computer (or TV).