FAMILY RESOURCE

CYBER SECURITY AT HOME

CYBER SAFETY PROJECT

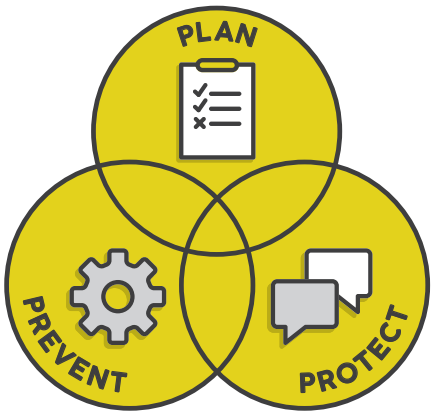
cybersafetyproject.com.au

CREATING A SAFE DIGITAL ENVIRONMENT AT HOME

The Cyber Safety Project are on a mission to empower every young Australian to self-manage their own cyber safety and digital wellbeing through proactive education.

We live in an era where technology is now an integral element of modern life. Advances in new technologies and devices are rapidly transforming how we live, learn, connect and play. When new capabilities emerge, new possibilities are created. These are also balanced with possible cyber risks and impacts to personal security, safety and wellbeing.

When it comes to using technology at home it's important to **plan** for device use, leverage tools and settings to **prevent** harms, and **protect** young people as they develop skills to safely and independently navigate the online world. Parenting in the 21st Century isn't easy but we've got your back. This Cyber Security at Home Guide has been designed to support parents, grandparents, guardians and carers with strategies to create a safe digital environment at home.



PLAN
Do your research, build awareness and set boundaries.

PREVENT
Make use of device, app and game settings.

PROTECT
Chat regularly and monitor your child's technology use.

WHAT ARE WE PROTECTING YOUNG PEOPLE FROM?

THE SHORT ANSWER: PEOPLE

STRANGERS

Just like in the real world, there are many users online who may be lurking in spaces to commit child exploitation. Unfortunately, it is easy to 'pretend' online and young people are at risk of the behaviour of strangers from the safety of their own home.

UNKIND PEOPLE

Negative comments and cyberbullying by online trolls or even those known to them, young people are exposed to a range of harmful communication.

TRICKY PEOPLE

Cyber criminals use many techniques and methods for personal gain. As digital users we must leverage all tools available to mitigate and eliminate those risks.

This guide provides important security fundamentals to help protect your family when navigating the digital world.

WRITTEN BY TRENT RAY & LUCA GENNAI

YOUR PERSONAL DATA

Hackers and malware look for data that can cause some sort of financial benefit for the person on the other side of the hacking or scam. They usually try to collect as much information as possible before making a move. Data can vary from the following:

- Birthdates
- Names
- Home addresses
- Habits
- Email addresses
- Passwords
- Tax File Numbers
- Contacts
- Family names
- Daily online habits and hobbies
- Banking information
- Medical Information
- Family trees and family linking

With access to some of this personal data, cyber criminals have the capability to impersonate you online. This can be over the phone or in person as they can be questioned and support claims with the information they've gathered. This can lead to:

- Identity theft (potentially multiple times)
- Contractual issues
- Financial losses
- Your private information being sold on the dark web
- Money being spent on devices due to them being infected with viruses or malware
- Loss of information
- Stalkers
- Future financial problems
- Family Stress
- Susceptibility to other attacks in the future

YOUR HOME WI-FI / MODEMS

Protect your family with the devices you are already using by making the most of your home Wi-Fi network and modem

Create a guest network: Having a guest network set up at home will allow visitors to connect as "guests" on your home network and can be a preventative measure to protect your Wi-Fi connected devices. This can prevent viruses, malware or bugs that they may have from entering onto the network your devices use.

Wi-Fi Network Names: Change your Wi-Fi network name from the default name it came with. Some modems (for example, "Telstra-B1234") can be easily identified as a home network. Changing to something like "Toxic-WiFi" can deter people from connecting. DO NOT use names like "JohnSmithsWiFi" or "Alice+Julie" that can be easily identifiable and give personal information away.

Wi-Fi Passwords: Usually, once a smart device is connected to the Wi-Fi network it will remember the password. Make sure the password is complex, hard to guess and has no personal information like names of pets or children. If setting up multiple Wi-Fi networks around the house, remember to have different passwords for them all. Passwords should include capital letters, lowercase letters, numbers and special characters. (A-Z, a-z, 0-1, !@#$%^&*).

Two-Factor Authentication: Where possible, it is always recommended to set up two-factor authentication for access to accounts. Two-factor authentication allows an extra layer of protection when logging onto accounts by sending a one-time code after the password is entered correctly to a pre-registered email or phone number. Due to hackers getting smarter, passwords can be easily guessed by software programs. If your password is hacked, the two-factor authentication will alert you when a code is sent to your phone number. If you receive an alert through two-factor authentication and you haven't been trying to access your account, it's always recommended to change your password to avoid being compromised.

Wi-Fi Encryption: When setting up or buying a modem, select WPA2 or WPA3 as your encryption. This is the strongest encryption available to protect your internet traffic. With WPA2 or WPA3 encryption turned on, each time you visit the internet your visit is encrypted, making it more difficult for hackers or eavesdroppers from seeing the data (username, password, credit card information, or other sensitive data) you're sending over the internet.

Smart Home Devices: Smart home devices such as Smart Speakers, Smart TV's or Smart Assistants should be set up on a separate network from the network you use to connect your phones, computers and other personal devices. Most smart home devices do not have a high level of security inbuilt into their system. Cyber criminals may attempt to infiltrate a home network through a smart home device. It's important to know that most smart home devices only connect to 2.5Ghz Wi-Fi networks and not 5Ghz networks.

Parental controls for limiting online time: Did you know that many modern modems come with parental control features? Your modem may allow you to restrict when devices are able to connect to your Wi-Fi network. This can be done in hour and minute blocks and you can even select specific days of the week. For example, restricting an iPad from using the internet between 7pm and 5am, or only allowing online use on Saturdays and Sundays.

Parental controls for site blocking: You can block particular websites from being visited by anyone on the Wi-Fi network. This can even be limited to specific devices (e.g. kids' devices). Some modems allow for this by setting URL rules. You may choose to block specific website links. Some antivirus software may also guide you during set up by blocking sites with categories such as explicit content or sites that allow webcam use (for example).

YOUR FAMILY'S DEVICES

Make the most of safety features and functionalities embedded in your personal devices.

SOFTWARE AND OPERATING SYSTEM UPDATES/CHECKING FOR UPDATES

An important step in keeping your personal devices safe, and not susceptible to cyber threats, is to perform all recommended software updates. When a recommended update is released, its purpose is to fix bugs found in its previous version. These bugs can relate to performance issues as well as security issues which can put the user at risk. Updating your software will allow for better and safer experiences for the user.

SETTINGS FOR SUCCESS

Navigate to the privacy settings on your device. Most hardware today has inbuilt security and safety features, but they are just not always set as default. Look for options to switch off location settings, local network configurations and password autofill.

DELETING THE UNWANTED AND UNNEEDED

Just like filing cabinets, devices can start to fill up with files, photos, videos and unused/unwanted apps that are no longer needed. By doing regular clearing, it can save storage space as well as allow your device to run smoother and more efficiently. Consider an external storage device/hard-drive and creating back ups of your files.

YOUR PROTECTION

Three non-negotiables to protect your family from cyber crime and digital harms.

ANTI-VIRUS PROTECTION

Anti-Virus solutions are readily available with solutions offered by hundreds of companies for free or for a very low, cost-effective price. These can be paid either monthly or yearly.

Many operating systems such as Windows or iOS now have inbuilt anti-virus protection as standard.

WHY IS ANTI-VIRUS PROTECTION IMPORTANT?

Anti-Virus software is designed to protect and defend your devices from infections of viruses, malware, phishing attacks, spamware and many other nasty cyber threats. They also protect your data that is stored on your device from being hampered with. Anti-virus software will often work in the background to scan new documents, links, photos or videos to evaluate if they are safe to be opened and aren't at risk of infecting your device. Some off-the-shelf anti-virus software solutions also include multiple extras such as firewalls, parental control functionalities, VPN's, system optimisers, password organisers and ID security.

FIREWALLS

Think of a firewall as a gatekeeper that allows good traffic in and blocks bad traffic out. Firewalls are a 'must have' for protecting yourself from the nasties of the online world. They are often included in anti-virus plans or subscriptions.

HOW DO FIREWALLS HELP YOU AND YOUR FAMILY?

Firewalls are important when it comes to stopping unauthorised access to your home network. They prevent people or other computers/machines accessing your private network, including other devices on that network. Without a firewall, all network traffic – the good and the bad – will be able to enter your network. This can then lead to viruses and malware establishing within your network and attacking devices in your home (tablets, computers laptops or phone).

VPN'S

VPN's or **VIRTUAL PRIVATE NETWORKS** allow you to browse safely on the internet. It masks your IP address and allows you to act privately online and makes it virtually impossible to track back to you.

VPN's also establish secure and encrypted connections for even greater safety online. Beware that your device can still get infected whilst using a VPN.

HOW CAN VPNS PROTECT YOU WHEN USING PUBLIC WI-FI?

Using a VPN when connected to a public Wi-Fi network such as in a shopping centre, airport, hotel or café, will help in stopping your private data being input online such as transactions, personal data, passwords and confidential emails/documents being eavesdropped by malicious strangers on the same network. The data you input will be encrypted and add that extra layer of protection.

Be aware: VPNs can also help your children access blocked content on your home network. One way to really make sure your child isn't using a VPN to bypass the blocked content you have set up for them is to create administrator passwords or accounts that require a password before download or installation. If you notice your child bypassing blocked content with a VPN, it is always best to check-in with them to understand why they are trying to do so and help them understand why the content is blocked for their safety.

GLOSSARY

WPA
Wi-Fi Protected Access (WPA) is an encryption used to protect Wi-Fi networks.

VPN
Stands for Virtual Private Network. When used, they help keep a user's connection secure.

MALWARE
An intrusive software that is designed to damage and destroy computers and devices systems.

VIRUS
A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

ENCRYPTION
The process of converting information or data into a code, especially to prevent unauthorised access.

FIREWALL
Protection (network or system) from unauthorised access.

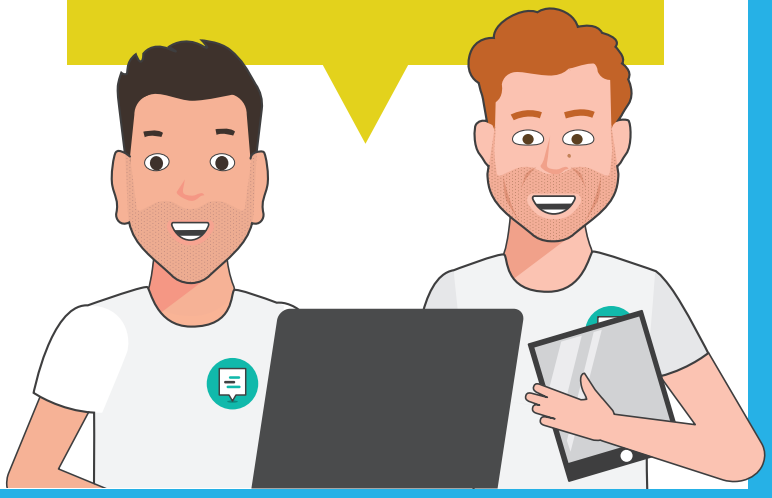
IP ADDRESS
An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol".

PHISHING
Phishing is a type of social engineering attack often used to steal user data, including log-in credentials and credit card numbers.

URL
URL stands for Uniform Resource Locator. Most people know it as a link which is able to direct you to an intended destination. Just like this URL: **www.cybersafetyproject.com.au** which will direct you to Cyber Safety Project's home page.

For more free resources, and information about our family workshops & webinars visit the Cyber Safety Project website

cybersafetyproject.com.au



CYBER SAFETY PROJECT

FIND OUT MORE

1300 114 117
info@cybersafetyproject.com.au
cybersafetyproject.com.au

trusted eSafetyprovider
esafety.gov.au