Protecting Yourself From Online Crime

Online Risks

The Internet has made it easier to communicate, bank and shop. Yet despite these advantages, technology is not 100% secure.

- Other people may use your devices or they may be lost or stolen
- Your device may be infected with a virus or other malicious software (malware)
- Public computers or networks may not be secure
- You may accidently disclose information online.

Online crimes may include:

- The illegal use of your personal details *(Identity Theft)*
- Dishonest online sellers - e.g. through sites like eBay *(Online Auction Fraud)*
- Fraudulent get-rich-quick schemes *(Scams)*
- Theft of financial details *(Credit Card Fraud, Phishing)*.

Follow these simple measures to help make sure you are communicating, banking and shopping safely online:

Checklist for Protection	*Tick*
Keep your devices in a safe place	☐
Install apps for locating stolen mobile devices	☐
Record your device model and serial numbers on a property inventory form, and mark devices with 'V' followed by your driver's licence number eg. V123456	☐
Ensure your internet or Wi-Fi connection is password protected and private	☐
Install up-to-date anti-virus and anti-spyware software and install and use a firewall	☐
Allow automatic updates on your software	☐
Use a secondary email address for non-private purposes	☐
Cover your webcam when not in use	☐
Backup all data regularly (USB, hard drive)	☐
Erase hard drives before disposing of a device	☐
Avoid using public computers for online shopping and banking	☐
Delete suspicious emails, and don't click on links or download anything sent from people you don't know	☐
Make separate, strong passwords for different applications – use numbers and symbols	☐
Don't allow the computer to save passwords	☐

Key Crime Prevention Tips

- **Secure** your physical devices and Internet connection
- **Install** anti-virus, anti-spyware software and use a firewall
- **Think:** Exercise caution when sharing information and remember, *If it sounds too good to be true, it probably is*

Online Shopping

- Shop only on reputable websites
- Check for the closed padlock symbol which shows it is a secure site
- Use a secure third party payment facility
- Read the terms and conditions before paying

Victorian consumer protection laws may not apply for online and international purchases.

Online Banking

- Banks **never** ask for your banking details in emails – do not open. Report and delete
- Never provide your bank details over e-mail
- Always log off when you are finished
- Regularly monitor your account transactions
- Only download and use mobile banking apps from the official website of your financial institution rather than general app stores.

Social Media

- Limit the amount and type of personal information you put online
- Set the security and privacy settings to limit access to your account and check the settings regularly.

Additional Resources

- Stay Smart Online – Australian Government: www.staysmartonline.gov.au
- Cybersmart – Information for children and families: www.cybersmart.gov.au
- SCAMwatch – provides detailed information about current scams: www.scamwatch.gov.au
- Consumer Affairs Victoria provides information about online shopping: www.consumer.vic.gov.au
- Contact your financial institution for additional security information about online banking.

VICTORIA POLICE

State Government Victoria Department of Justice

If you require immediate police attendance, call police on Triple Zero (000)
If you have any information regarding a crime, call Crime Stoppers on 1800 333 000
For further crime prevention information, visit the Victoria Police website at: **www.police.vic.gov.au**
Visit the Victorian Government Community Crime Prevention Website at: **www.crimeprevention.vic.gov.au**