Tips for Tech Savvy Seniors

Introduction to Cyber Safety

Intermediate Guide

The internet comes with some risks, but there are some simple rules and commonsense behaviours you can follow to protect yourself and help keep yourself safe online.

The threats you might face

For most internet users, the three key dangers to be aware of online are malware, hackers, and identify theft.

- **Malware** (malicious software) accesses your computer and may steal personal info, wreck your files, or put ads everywhere. Usually, malware tricks the user into downloading and installing it.
- **Hackers** are people who try to break in to your computer using a security flaw or by tricking you into giving access. Hackers may steal or delete your files and sell your personal information such as banking details.
- **Identity theft**, **phishing**, and **scams** rely on you not knowing who you are talking to online. They will contact you via telephone or message and try to convince you to give them money.

NSW
GOVERNMENT

How to spot phishing emails

You can usually identify an email as a phishing attempt or spam, if it has any of the following signs:

- A name in the **From** field you don't recognise, or a **subject** you don't remember signing up for
- An **offer of free money** in exchange for your personal information
- Warning of consequences if you don't **click** a link in the email right away
- A **To** field that is just blank, instead of containing your name and email address
- Looks like it has come from a bank or other large organisation, but has lots of spelling and grammatical errors
- Has an address in the **From** field that's from a free service, such as Yahoo or Gmail
- Says you are a good or important person, and asks for help with something, in exchange for lots of money. This is an example of a **vanity scam**.

Protecting your computer with security software

Computers come with security software built-in, and you can add more for extra protection.

- **A firewall** is like a security checkpoint for internet traffic. Apps on your computer are restricted in how they talk to the internet, and vice versa. You can choose which apps are blocked by the firewall, and which are allowed online.
- **Antivirus** software scans your computer and identifies known viruses and malware, and removes them before they can do any damage.
- **Parental controls** let you restrict certain websites and limit how much time a computer can use the internet per day.
- **Backup software** saves your important data to external storage.
- **Spam filters** detect spam emails and stop them getting to your inbox.
- **Web filters** block websites that have been identified as scams.
- **Identity Theft Protection** stops your personal information from being sent over the internet.

Once you install protection software, it runs in the background. You can click the icon in the bottom right of the screen to see a security panel, including controls to scan for malware manually. If a threat is detected, the software will show a pop-up with information about what to do next.

Keeping yourself safe

Remember to stay alert to scams and be sensible about what data you share over the internet. Other safety tips include:

- Use a strong password and change it regularly
- Use more than one kind of security
- Set up two-factor authentication (2FA) where possible
- Use a password manager
- Keep your device up to date
- Don't post personal information on public sites
- Don't open email attachments unless you are sure they are safe
- Never respond to a scam or fake email
- Keep your credit card details close, and use secure payment systems like PayPal
- Don't install apps from untrustworthy sources
- Run a Google search on a website name to see if Google has identified it as a known scam site
- When you download an app, run a virus scan on it before installing it on your computer.

What happens if a threat is detected?

Your computer will show a warning panel, usually in the bottom right or top left of the screen:

- The panel will identify the threat and block it
- Your security software will offer to remove the threat automatically (you should say yes)
- A summary page will show some technical information about the threat and say the threat has been removed.