Scouts
VICTORIA

IN PARTNERSHIP WITH

Psyber

ONLINE SAFETY GUIDE

Cyber Safe eBook

Protect your security at work, at home, and everywhere in between.

Introduction

Scouts have always been taught to "Be Prepared."

In today's digital world, that means being prepared online too. As technology and AI become woven into everything we do, so too does the growing risk of cybercrime. Now, more than ever, implementing safe online habits is crucial. It's part of looking out for ourselves and the people around us.

This eBook is a practical, simple guide to help you, your family, and our scouting community stay safe and confident online.

WHAT'S INSIDE

WHY DOES THIS MATTER FOR YOU?

> 90%

of all cyber attacks are a result of human error.

There's a common misconception that cyber attacks are the result of sophisticated hacking. The reality is, most cyber attacks start with **people.** Someone clicking a fraudulent email, reusing a stolen password, or downloading a virus. Cybercriminals know that targeting people is much easier and more effective than breaking into technology.

At Home

- ✓ Protect your financial information, money and personal data by keeping accounts secure.
- ✓ Prevent your identity being stolen and used by cybercriminals.

At Scouts

- ✓ Help Scouts Victoria keep its confidential information safe.
- ✓ Help maintain its reputation as a secure and trustworthy organisation.

Spot Scams

Cybercriminals use the internet to scam unsuspecting victims. The most common technique used to compromise your information is **phishing,** and it's getting more sophisticated.

> **PHISHING**
>
> A scam where cybercriminals trick you into giving out personal, financial or business information. This can be used to steal your money, your access or your identity.

Phishing messages copy the branding of organisations you know and trust, or impersonate someone close to you, a colleague, a friend, or even a family member. Attackers know we're far more likely to act when a message comes from someone we trust.

✓ `www.scoutsvictoria.com.au`

✗ `www.scoutssvictoria.com.au`

Don't take the bait!

To catch a phish, always look out for **SHARK**.

- **S** — **Sender**
  Are they really who they say they are?
- **H** — **Heightened Emotion**
  Are you pressured into action?
- **A** — **Analyse Language**
  Does the tone and wording feel right?
- **R** — **Requests**
  What are they asking you to do?
- **K** — **Know**
  Pause and verify before taking action.

DELIVERY METHODS

Email phishing	Fraudulent emails designed to trick you into clicking a link, opening an attachment, or handing over information, often by impersonating a trusted organisation or person.
SMS smishing	The same tactic, delivered by text message. Attackers impersonate banks, delivery services, or government agencies to get you to act.
Voice Call vishing	A caller pretends to be someone you trust, such as your bank or the ATO. They use real-time conversation to gain information or obtain remote access to your device.
QR Code quishing	QR codes can't be previewed, and attackers exploit that. Scanning a malicious code can redirect you to a fake website designed to steal your information.
Social Media	Attackers use platforms like LinkedIn, Facebook, or Instagram to contact you, impersonate someone you know, or share malicious links.

Protect Your Information

Passwords are out, passphrases are in.

7,000

password-based attacks are blocked by Microsoft every second.

Attackers relentlessly target passwords because they unlock everything: your bank account, your identity, even your friends and family if your accounts are used to impersonate you. Yet most people still don't practice strong password habits. They reuse passwords that have been compromised, or build them from personal details, like a pet's name, a birthday, a favourite team.

MAKE IT A `l0ng, $tr0ng & m3m0r@ble p@ssphr@se`

Rather than setting and reusing simple passwords, we recommend a **passphrase** as a stronger alternative. It's a sequence of random words that is long enough to be hard to crack, but easy enough to remember.

DO THIS

- ✓ Create a long, strong, memorable passphrase.
- ✓ Use a different password for every account.
- ✓ Use a password manager to store them securely.
- ✓ Turn on MFA and use an authenticator app.

NOT THIS

- ✗ Reuse passwords across your accounts.
- ✗ Use words associated with your identity.
- ✗ Write passphrases down or store them on your device.
- ✗ Share your password with anyone, even your team.

Check whether your accounts have been compromised at **haveibeenpwned.com**, and set up alerts for the future.

MULTI-FACTOR AUTHENTICATION

Businesses are breached every single day, which means it's only a matter of time before your password ends up in the wrong hands. That's why MFA is crucial. It confirms you're really who you claim to be at login, requiring more than one method of verification. Even if your password is compromised, MFA stops attackers in their tracks.

99%

of automated attacks are blocked by MFA.

Something you know

Password PIN Key

Something you have

Token generator

Something you are

Fingerprint Face / retina Voice

Protect Your Devices

Your device is the front door to everything else, your accounts, your messages, your photos, and Scout information. A few simple habits make it much harder for an attacker to get through.

Lock it before you leave it

Locking your screen whenever you step away, at home, at work or anywhere in between, is simple but vital. An unlocked, unattended device gives anyone access to the sensitive information you handle. See an unlocked screen? Give the person a friendly reminder.

Update your software

Updates don't just add features, they fix vulnerabilities and remove security bugs that criminals exploit. Install updates as soon as possible, or enable automatic updates.

Back up your devices

Documents, contacts, photos and emails are invaluable. Regular backups to an external drive or the cloud protect your data if a device is lost, stolen or infected.

Be careful on public Wi-Fi

Public Wi-Fi at cafes, airports, or events, aren't always what they seem. Attackers can set up fake networks designed to look legitimate, and once you connect, they can intercept what you do while connected to that Wi-Fi. Where possible, use mobile data instead.

QUICK CHECKLIST

- ✓ Lock your screen every time you step away.
- ✓ Back up your devices regularly.
- ✓ Turn on automatic software updates.
- ✓ Avoid public Wi-Fi where you can.

TRAVEL SECURELY

Always consider the risks to information stored on your devices when they're used overseas. Different countries have different rules, and unfamiliar Wi-Fi networks can carry extra risk, so plan ahead and take only what you need.

Pack light, stay alert, back up before you go.

While travelling

- ✓ Keep devices within reach at all times.
- ✓ Take essential devices only.
- ✓ Avoid banking on unsecured networks.
- ✓ Don't use public USB charging kiosks.
- ✓ Enable location tracking and back up your data.

Protect Others

We share information every day. Exercise caution and understand how what you share can affect your family, friends or Scouts Victoria if it falls into the wrong hands.

At Home

- ✓ Limit the personal information you share online, such as your home address or phone number.
- ✓ Reduce the photos you share, any photo online can be accessed and reused by others.
- ✓ Google yourself to understand your digital footprint and what already exists online.
- ✓ Set up Google alerts so you're notified if your name appears in the media or a post.

At Scouts

- ✓ Only share data on a "need to know" basis, and use the right channels to do so.
- ✓ Always verify the recipient and check the email address before you send sensitive information.
- ✓ Never forward Scouts documents or emails to personal email addresses.
- ✓ Avoid inserting USBs or storage devices of unknown origin.

PROTECT YOUR FAMILIES

Children

94%

of 8–18 year-olds have access to a smartphone.

340%

increase in complaints to the eSafety Commissioner.

Help your children safely navigate the digital world. Your support and guidance gives them the confidence to make safe decisions online and to ask for help when they need it.

- ✓ **Access controls** — set age-appropriate rules, use parental controls, and check app age ratings.
- ✓ **Set boundaries** — agree rules together, and consider a family tech agreement (with rules for parents too).
- ✓ **Openly communicate** — ask about their experiences, get involved, and reassure them they can always come to you.

Seniors

30%

of online fraud victims are aged 65+.

$27M

lost by seniors to fraud between January and June 2026.

Cybercriminals target seniors more than any other age group. This is because they know they have more accumulated wealth than any other demographic, and are perceived to be less experienced with technology.

- ✓ Foster regular discussions about scams and online risks.
- ✓ Help them set up MFA, update devices and create strong passphrases.
- ✓ Warn them: unsolicited contact that seems "too good to be true" usually is.
- ✓ Direct them to the right channels for reporting if they're caught out.

Where To Get Help

Despite your best efforts, sometimes things don't go to plan. When it comes to cybersecurity incidents, speed matters. The sooner you act, the more that can be done to limit the damage. Here's what to do, and who can help.

IF YOU'VE CLICKED A PHISHING LINK

Just clicked?

- ✓ Close the webpage immediately.
- ✓ Don't enter usernames, passwords, MFA codes, or payment details.
- ✓ Don't download any files or allow browser notifications.
- ✓ Run a malware scan using your antivirus or security software.
- ✓ Monitor your accounts for anything unusual over the next few days.

Entered your data?

- ✓ Change your password immediately on all accounts you've used it.
- ✓ Enable MFA.
- ✓ Check recent login activity and sign out of unknown devices.
- ✓ Contact your bank immediately, and freeze or cancel cards if advised.
- ✓ Monitor transactions closely and report any unauthorised activity.

Downloaded something?

- ✓ Disconnect from the internet if you suspect malware is being installed.
- ✓ Run a full antivirus scan.
- ✓ Contact your IT team immediately if it's a work or Scout device.
- ✓ Contact Scouts Victoria if it's a device you do scouting on.
- ✓ Watch for signs of compromise, such as unexpected pop-ups, new programs, or unusual activity.

REPORT IT

- ✓ Report the scam to **Scamwatch** (run by the National Anti-Scam Centre).
- ✓ If your money, card or account details have been exposed, call your bank immediately.
- ✓ Report suspicious emails to the **Scouts Victoria** IT team at **m365.support@team.scoutsvictoria.com.au**.

IF YOUR IDENTITY IS COMPROMISED

IDCare

If your personal information has been stolen or misused, i.e. your ID documents, Medicare details, or bank information, IDCare can help. They're Australia and New Zealand's free, independent identity and cyber support service. Call them and they'll talk you through exactly what to do next based on what's happened to you.

PHONE **1800 595 160**

ONLINE **idcare.org**

! **Speak up.** There's nothing to be ashamed of if something's gone wrong. The faster you raise it, the faster it can be contained, for you, your family, and Scouts Victoria.

STAY ONE STEP AHEAD

Cybersecurity isn't a one time task, it's a daily mindset.

Every action you take, from locking your device, using a strong passphrase, to questioning a suspicious message, builds a more secure future for yourself and your family. Cybercriminals rely on us being distracted or unprepared. With knowledge, good habits and the right support, we can all stay one step ahead.

Scouts VICTORIA

IN PARTNERSHIP WITH

Psyber