GET SET UP FOR SAFETY

Secure your devices

A scam is a made-up story to trick people out of money or steal their information. Learn how to check for red flags.

SPONSORED BY

CHORUS | netsafe

Discover your settings and learn how to change them to enhance your privacy and security.

Topics

Secure your devices checklist

01

Set up a strong, unique password for each device and online account

Strong passwords use a long mix of numbers, letters, and symbols. Strong passphrases use four or more random words, like nanashouseiscool or stayoffmybluesuedeshoes. You can mix it up a bit, like 1willsurviveTinaTurner.

Safe password habits

- Avoid using personal information in your password. It is too easy to guess. Personal information includes your name, birth-date, address, family members or pet's names.
- Keep your password to yourself.
- Use a secure online password manager to help you remember all your passwords.

How do I set passwords on my device?

Android devices

- Go to ‘Settings’.
- Click ‘Security’.
- Go to ‘Change Screen Lock’ (the phase will vary on each phone).
- Choose a password, pin, pattern or even your fingerprint as a secure method to unlock your phone.
- Once you set your security option, decide on when you want the phone to lock itself e.g., after 30 seconds of inactivity.

Apple devices

- Go to ‘Settings’.
- Your phone will have either ‘Face ID & Passcode’ or ‘Touch ID & Passcode’.
- Select ‘Passcode On’ or ‘Change Passcode’.

Having a strong password is a good starting point to secure your accounts. The next level of security for your accounts is to use two-factor authentication.

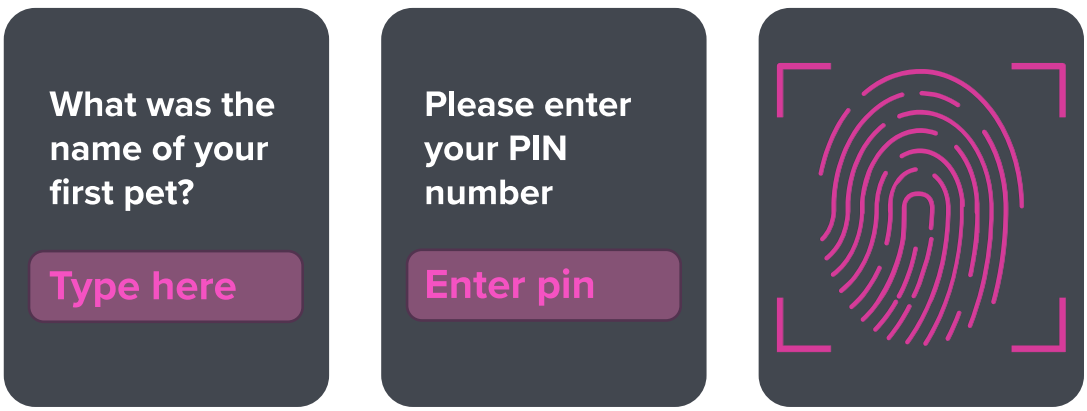
02

Use two-factor authentication for your online accounts

Two-factor authentication (2FA) is also known as multi-step verification or login approvals.

Turning on 2FA for your online accounts adds an extra security step to the login process; in addition to your password, you also enter a second piece of information. It's like using two padlocks on a gate - only a person with both keys can unlock the gate and gain access. Using 2FA makes it harder for unauthorised people to get into your accounts.

You often have the choice of what the extra security step looks like.



CHORUS | netsafe

02 Use two-factor authentication for your online accounts

For example, you may be able to answer a security question, use your fingerprint, or have a code sent via text/SMS to your mobile phone.

You can set up 2FA on your device and most of your online accounts, such as:

Email accounts

Social media accounts

Internet banking

Online shopping sites

- Once you've logged in, go to security settings.
- Turn on two-factor or multiple-factor authentication.
- Choose the security method you want to add, and follow the on-screen instructions.

Watch a video on how 2FA works by visiting netsafe.org.nz/older-people

03

Your device settings

There are some basic settings that you should choose to set your device up for safety. To change your settings, look for the settings menu on your device. It may look like:

Set your screen to lock automatically and always lock it when not using the device.
Locking your screen keeps your information more secure and protects your privacy.

Install software updates on your device and set your device to update automatically.
Updates often include new security features which can fill security gaps on your device. Setting your device to update automatically means you don't have to remember to do it everytime your device tells you there is a new update! Go to your device settings and turn on automatic updates.

Protect yourself from harmful emails by blocking spam

Spam is any unwanted email that you haven't asked for or signed up to. Usually these unwanted emails are sent in bulk to many people at once.

- Turn on spam filters in your email app. Go to the support page on your email provider's website and search 'spam'.
- Turn on spam filters on your phone.

Android devices: Go to Settings > Spam Protection. Make sure Enable spam protection is toggled on.

Apple devices: Go to Settings > Messages > Message Filtering. Turn on Filter Unknown Senders. This will filter all messages from unknown senders into another folder and you won't be notified about them.

In addition to turning on spam filters, avoid clicking on links or opening attachments in emails or messages you weren't expecting. This can help you dodge scam messages containing information that can harm your computer or attempt to capture your personal or credit card information.

04

Your app settings

Set your apps and social media accounts up for security and privacy.

Some settings need to be done inside the app or social media account that they apply to.

- Open the app or login to your social media account. Look for the privacy and security settings menu.
- Read through the options available on each platform. For example, on Facebook you can ensure you have a private profile and you can limit or amend your audience for each post.
- Consider carefully what information you want to share and who you want to share it with and adjust the settings accordingly. For example, do you want to share photos of your grandkids with the public, your social media friends, or just family?
- Check your settings regularly as platform updates in the background may change the options available.

05

Your software

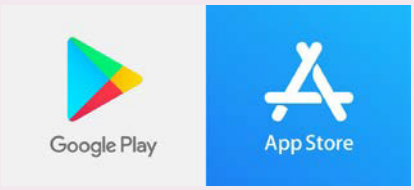
Install antivirus software on all devices and keep it up-to-date.

Antivirus software will help to block malware like viruses and spyware. If your software is alerting you to something, remember to follow up on what it's asking you to do or ask someone for advice - don't ignore the message or turn it off.

Before downloading a new app, check its reviews and what permissions it requires

Stick with the official marketplaces to avoid installing malicious software and be cautious about what permissions are requested during the installation process. Does that free game really need to be able to read or send text messages or access your camera?

Official marketplaces



CHORUS | netsafe

06

Your web browser settings

A web browser is software you use to access information on the internet.

You can tell when you're using a web browser because there will be a web address (also called a URL) at the top of the page e.g. https://netsafe.org.nz.

https:// - Set your web browser to search only on secure sites

Some sites online are more secure than others. Sites with a web address that starts with 'https' encrypt your information, while sites with just an 'http' web address do not.

Remember, while the 'https' means your information is encrypted, it doesn't necessarily mean that the person or organisation running the website is legitimate. You will still need to be careful about any information you choose to share.

Change your web browser settings to only show search results from websites with ‘https’.

Google Chrome

- Settings ⋮ (vertical three dot menu on top right) > Privacy & security > Security.
- Scroll to bottom > Toggle “Always use secure connections”.

Mozilla Firefox

- Settings > Privacy & Security.
- Scroll to Bottom > Enable HTTPS-Only Mode.

Safari – this is set by default in Safari 15.
No setting changes are needed from the user.

Microsoft Edge

- To switch on Automatic HTTPS in Edge, type edge://settings/privacy in the address bar and hit Enter.
- Scroll down, and under Security, turn on the toggle for Automatically switch to more secure connections with Automatic HTTPS.

Block pop-up ads

Ads or windows that pop-up are annoying, but can also contain harmful scams. Set your browser to block them.

Google Chrome – On your computer

- Open Chrome.
- At the top right, click three dots > Settings.
- Click Privacy and security Site Settings. Select pop-ups and redirects.
- Don't allow sites to send pop-ups or use redirects.

Mozilla Firefox:

- Click the menu button and select Settings.
- Select the Privacy & Security panel.
- Go down to the Permissions section.
- Check the box next to Block pop-up windows to enable the pop-up blocker.
- Click the Exceptions… button to the right of Block pop-up windows to open a dialog box to choose which sites are allowed to display pop-ups.

Block pop-up ads

Safari – On your Mac

- Open Safari and choose Safari > Settings (or Preferences) from the menu bar.
- In the Websites tab, you can configure options to allow or block some or all pop-ups.
- Turn on the fraudulent website warning setting in the Security tab

Safari – On your iPhone or iPad

- Go to Settings > Safari.
- Turn on Block Pop-ups. You also have a setting here to Turn on Fraudulent Website Warning.

Microsoft Edge:

- Go to Settings and more at the top of your browser – look for the three dots ●●● .
- Select Settings > Cookies and site permissions.
- Under All permissions, select Pop-ups and redirects.
- Turn on the Block (recommended) toggle.

07

Secure your devices

Go through the following checklist to make sure your devices are as secure and private as possible. For information on how to action these checklist items go to netsafe.org.nz/older-people.

01	**General security**
✓	Set up a strong, unique password for each device and online accounts.
02	**Use two-factor authentication**
✓	Set up two-factor authentication for your device and online accounts.
03	**Your device settings**
✓	Set your screen to lock automatically and always lock it when not using your device.
✓	Install updates for all apps / software on your device and switch on automatic updates.
✓	Turn on spam filters in your email account and for your phone text messaging.
04	**Your app settings**
✓	Turn on security and privacy settings on apps and social media accounts.
05	**Your web browser settings**
✓	Install antivirus software on all devices and keep it up to date.
✓	Before downloading a new app, check the reviews and permissions.
06	**Your web browser settings**
✓	https:// - Set your web browser to search only on secure sites.
✓	Turn on ad blockers to prevent accidentally clicking on any harmful ads or pop-ups.

Additional resources

Explore our full range of Get Set Up for Safety in-depth guides, quick fact sheets and interactive learning activities for older adults and those that support them. There are over 20 to choose from, covering online safety and security topics including:

- Device & account security
- Scam awareness & response
- Social media & dating safety
- Emerging tech, accessibility and terminology

Visit netsafe.org.nz/olderpeople

If you're unsure about a situation or need further advice, you can find more information on the Netsafe website netsafe.org.nz.

We're here for you. If you require assistance or experience online harm, contact Netsafe.

Call 0508 638 723

Visit netsafe.org.nz

report.netsafe.org.nz