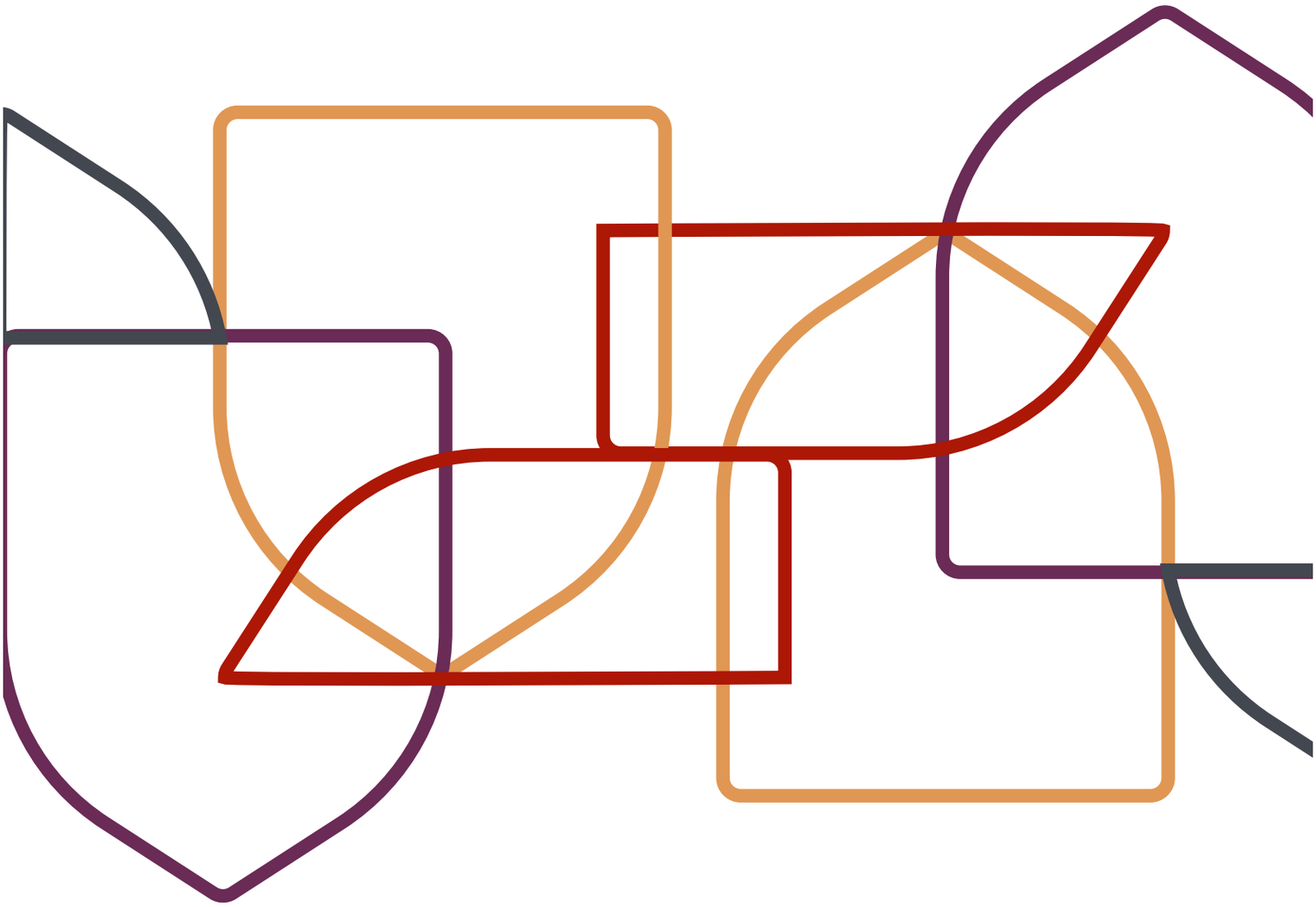
ONLINE SAFETY

Glossary

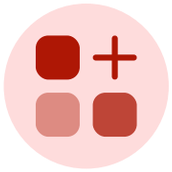


SPONSORED BY CHORUS

netsafe
netsafe.org.nz

Contents

Stay up-to-date with digital terms using Netsafe's glossary. Having an understanding of these terms means you can stay safer online.



App

a type of software on an digital device. Check your app permissions on your device to limit the personal information collected and shared about you.

Attachment

An email attachment is a computer file, document or picture sent with a message. Before opening an email attachment, think about whether you are expecting this file and if the sender is someone you know and trust.

Blocking

Blocking online means using technology or settings to prevent certain people or websites from reaching you or accessing your information on the internet. It's like setting up a virtual barrier to keep unwanted online interactions or content away.

Browsing history

Browsing history is a record of the websites and web pages you've visited while using the internet, like a digital trail of your online activity. It can be helpful for revisiting websites you've previously viewed or tracking your internet usage. Clear your browsing history regularly from the privacy and security menu of your browser.

Cookie

Cookies are small pieces of data that websites save on your computer when you visit them. They help websites remember your preferences and login information, making your online experience more convenient, but they can also be used for tracking your online behaviour.

Cyber or online bullying

Someone deliberately **and** repeatedly doing something that causes harm to another person online, with a mobile phone or other electronic device. Report bullying to the platform hosting the comments and to Netsafe. Use your platform security settings to block abusive individuals to protect yourself.

Digital footprint

This describes the traces of your personal information and activities as you use the internet. To understand your footprint, search your name online and see what's visible. Sharing content online means you can't always control who sees it, so think about your audience before sharing.

Download

Downloading transfers a copy of a digital file (such as a word document, pdf, or video) to your chosen device and is sometimes referred to as a 'download'. Before downloading and opening a file, ask yourself if you trust the source, and if you know what's in the file. It's worth checking the file type to see if it matches what you think is in the file e.g. if you think it's an information document, the name of the file should end with .pdf or .doc, etc.

E-wallet or digital wallet

A financial transaction app or platform that stores payment information and passwords (i.e. Google Pay, Paypal, Afterpay). Check reviews and only use reputable services for safer purchases.

Fraud

Wrongful or criminal deception intended to result in financial or personal gain. Be aware that not every story you see online is necessarily true. While most people are genuine, there are some people online who will tell false stories in order to manipulate you to get you to share money or personal information they can profit from.

Identity theft

The unauthorised use of someone else's personal information, usually for financial gain. Avoid sharing your personal information online – even basic information like your birthday and address can be used to impersonate you and commit fraud.

Internet or web browser

Software that's used to access and view information and websites on the internet. Look at your browser settings for options to make your web browsing safer.

Impersonation

Pretending to be someone else online, often done to gain trust and manipulate other people to share personal information and money. Be aware that not everyone you meet online is necessarily who they say they are.

Malware

Harmful software (e.g computer virus) that can damage, disrupt and take control of a device or steal personal information. To keep your device safer, don't open suspicious links or emails, only download apps or content from trusted sources, use an anti-virus programme and regularly update software and apps to keep your device safer.

Multi-step verification (two-factor authentication, 2FA)

This is an extra security step to pass before you can login to your account. It means in addition to a password you have to provide a second piece of information. This may be a PIN (personal identification number), fingerprint or temporary access code from a trusted device, etc. Set up two-factor authentication for your accounts to help keep them secure.

Online shopping

Purchasing or transacting online. Use trusted sites and sellers with good reviews, and only enter payment details into secure websites. Look for "https://" and a padlock icon in the address bar for safer online transactions.

Password

Secret code or phrase to protect accounts. Set strong, unique passwords or passphrases with capital letters, numbers and symbols for better security.

Personal information

Information about you that can be used to access your accounts, build a fake online presence or impersonate you including:

- login details and passwords to any online account including banking, email, social media and trading sites
- bank account and credit card details
- address
- phone number
- birthdate
- personal information linked to the security questions on your online accounts
- driver's license
- passport details.

Safeguard your personal information and limit what's shared online for added protection against fraud.

Phishing

Deceptive emails, messages, or websites designed to steal personal information or money from victims. To stay safer from phishing attempts, only open emails or messages from people you know and trust, and don't click links in messages. If you want to visit a website – look for it by using a search engine such as Google or Bing.

Pirating

Using a site to watch or read content for free that is usually paid for. Downloading (or streaming) music, movies, and TV shows for free is tempting, but it's best to avoid them. Websites that offer this service are generally unsafe, and they're often full of malicious links and malware downloads.

Platform

An online platform is a digital environment to connect people, communicate, learn, shop, or play. It can be a website or app that provides people with access to services or functions (i.e. social media platforms, e-commerce platforms, video platforms).

Public Wi-Fi

Public places may offer free wi-fi. Connecting to free networks can be risky as the network may not have security set up properly, which leaves your internet data vulnerable to being intercepted. Avoid sharing sensitive info while using public Wi-Fi hotspots, or use a VPN to secure your data while using these networks.

Scam

A scam is a made-up story to trick people out of money or steal their personal information. Use **SCAMS** to spot the most common red flags of a scam and take action: **S**urprise, **C**ontrol, **A**ccess to personal information, **M**oney requests. Be cautious about who you communicate with online, and never send money to anyone you don't know or haven't met in person. If you see a red flag or don't feel comfortable with a story, **S**top communicating, seek support from your whānau and contact Netsafe for next steps.

Social media

Online platforms where users can create profiles, share content, and interact with others. e.g. Facebook, LinkedIn, Snapchat, YouTube. Be cautious about sharing personal details and avoid oversharing on social networks to guard against identity theft.

Spam

Unwanted, unsolicited digital communication sent out in bulk. You can use email filters to block spam senders and create rules to send them directly to junk. Report all spam to the NZ Department of Internal Affairs – forward emails to complaint@spam.govt.nz; forward texts to 7726 and reply to the text response from the DIA with the phone number the spam message came from.
cert.govt.nz/individuals/common-threats/spam/

Suspicious links

When you hover with a cursor over links in messages, emails, or online, you may notice that the website URL that shows up doesn't match what the link says it should be. E.g. it goes to notsafe.org.nz instead of netsafe.org.nz. Don't click on suspicious links.

Two-factor authentication

(2FA, multi-step verification): See multi-step verification.

Virus

A type of malware that spreads by attaching itself to other files or programs and can cause damage or steal information. Be cautious about which computer files and email attachments you download and open.

VPN

Virtual Private Network. Download a VPN to encrypt data you send over wifi to make it safer to use unsecured public wifi networks. These are often included in anti-virus and security software packages which protect your device, such as Norton and AVG.

Web or internet browser

Software that's used to access and view information and websites on the internet. Look at your browser settings for options you can turn on to make your web browsing safer.

Additional resources

Now you're familiar with common digital terminology. Learn more on other Get Set Up For Safety topics by visiting **netsafe.org.nz/olderpeople**, including:

- **Staying connected**
  Learn the basics of social media platforms and how to adjust privacy and security settings to socialise online safely.
- **Spot a scam**
  A scam is a made-up story to trick people out of money or steal their information. Learn how to check for red flags.
- **A user-friendly device**
  Set up your device so it's easier and safer for you to use.
- **Safer shopping, banking and investing online**
  Learn how to avoid scams and what to do when things go wrong.
- **Secure your devices**
  Set up your devices (phones, tablets, PC's, etc.) for safety, to give you peace of mind when online.

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