It's 2024!
Take control of your digital safety

Te Whatu Ora
Health New Zealand

New beginnings, a fresh start, a reset…whatever you like to call it, the start of a new year is the BEST time to embrace new habits. Keeping information and devices secure from hackers or accidents is a lot to take in and takes time.

Home

Secure your home Wi-Fi

At home, use a secure Wi-Fi network with a strong password. Don't use the default one.

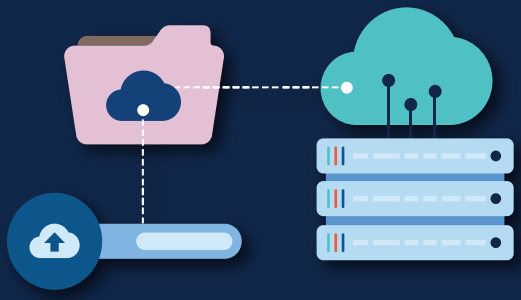
Make sure your Wi-Fi is encrypted (WPA2 or WPA3 is good).

If you travel a lot and use public Wi-Fi consider the use of a Virtual Private Network (VPN)

Get to grips with backing up!

Backing up your device means creating copies of your most important information and storing those copies in a different place. This could be in the cloud (for example, iCloud or Google backup) or a physical storage device like an external hard drive.

Backing up gives you peace of mind that you can access documents and photos if you lose your device or accidentally delete files, or your device is damaged.



Fingers crossed it never happens, but if your files are locked or accessed by a hacker or wiped by a virus, your back-ups will save the day.

Work

Become a champion phishing spotter

Email scams (phishing), phone call scams (vishing) and SMS text scams (smishing) aren't going away any time soon. Add AI generated phishing and voice-cloning to the mix and it's very hard to spot real from fake.

Am I expecting this link or attachment?

Am I feeling pressured to respond quickly?

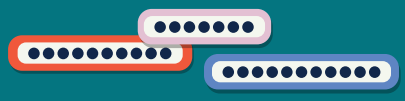
Does this email make me feel uneasy?

If you answer YES to any of these questions, report the email by clicking the 'Phish Alert' Button on your Outlook toolbar.

If you've shared personal or Te Whatu Ora information, stop what you're doing and contact your local helpdesk for support.

Browse the internet safely

Keep your work and personal online lives separate by having different logins for each online account. If a hacker got into a personal account which used your work login, they may try to access your work accounts too.



Avoid clicking on pop-ups and ads which could take you to a fake website where you could be tempted to enter personal information.

2024 is the year to become a pro at password management. Use separate passwords for all sites. Ensure they are strong and backed by MFA. Think about secure password management

It's 2024!
Take control of your digital safety

Te Whatu Ora
Health New Zealand

Start 2024 with these ESSENTIALS and you've set up a great foundation to build your personal and work security as the months roll over.

Home

Make technology and it's use safer with encryption

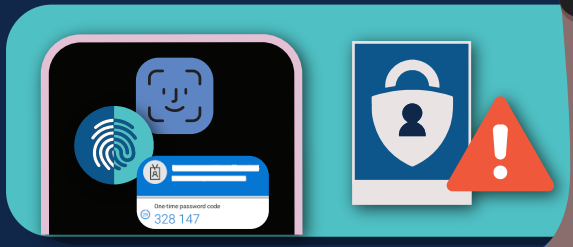
Encryption helps keep your online information safe. It hides certain information from everyone except the person you're communicating with.
It happens without you knowing on your banking and email.

Encryption scrambles info when it moves from sender to recipient so criminals can't access it, especially important or sensitive info.

Use apps from trusted sources with encryption enabled.

Secure your online accounts with multi-factor authentication (MFA)

When you log into an online account, MFA is the second layer of information you're prompted to provide to access your account. It could be a code from an authenticator app like Microsoft Authenticator, your voice, or your fingerprint – anything that's unique to YOU!



Turn MFA on when you sign up to a new online service, it's usually found in Settings > Privacy / Security.

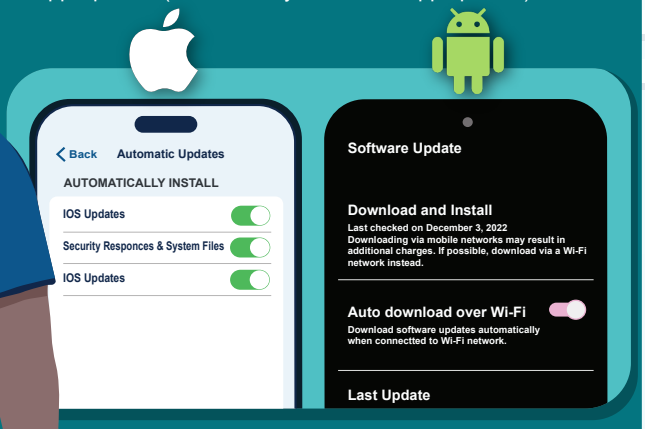
It's a great way to add extra security to your accounts as without YOUR phone, a criminal will find it very difficult to get to your information.

Work

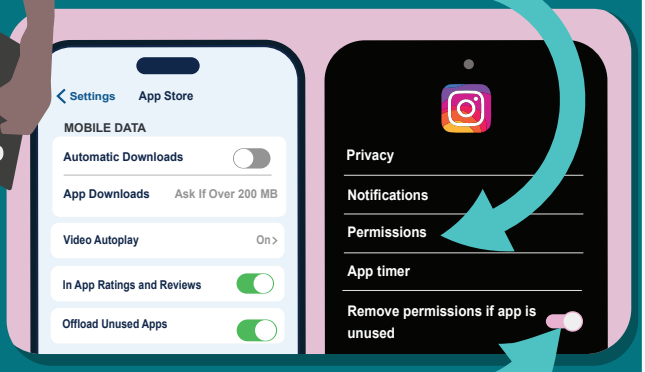
Take control of your device security

Proud owner of a new device? Make it your own and make it safe.

Set app updates to run automatically. Settings > App Store > App Updates (automatically install new app updates).

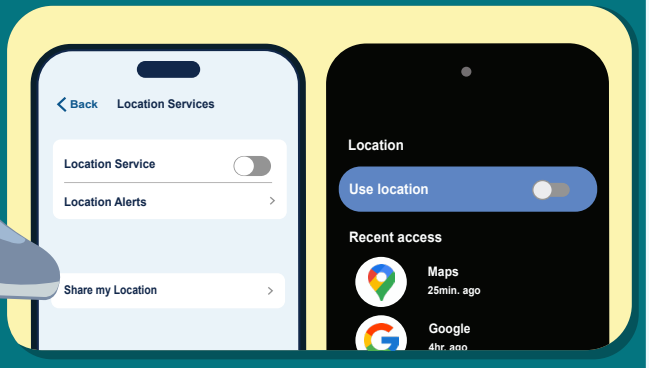


Review app permissions and turn off access to location, calendars, camera or microphone that aren't needed for the app to do what you need it to.



Uninstall apps you aren't using regularly.

Enable "Allow While Using App" option when turning on the location setting.



Power down your device from time-to-time for operating system (OS) and software updates to be installed. Restarting your phone may help malicious software (malware) from taking hold.