/// Get Cyber Smart

Enable two-factor authentication (2FA)

That's two ways of identifying who you are – it's usually by entering a code from another device on top of your password. 2FA adds an extra line of defence when you log in online.

Even if a hacker knows your password, with 2FA in place they still can't get to your accounts. You can use 2FA for most email, social media, banking and shopping accounts, as well as to access your devices. Every site, app or device does 2FA slightly differently. Look under your account or privacy settings or check the help section. It can also be called 'two-step authentication' or 'multi-factor authentication (MFA)'.

Turn on 2FA for all of your important accounts

Once it's set up it's as easy as entering an extra code when you log into a new device.

Keep your phone, device or hardware tokens safe

Treat your device like a password or your keys and keep them safe. Keep using good password practices, such as using unique phrases.

Watch for rogue codes

If you receive a code for an account you weren't trying to log in to, change your password - someone might be trying to access your account.

/// Get Cyber Smart

certnz connect SMART

Get more Cyber Smart tips at
cert.govt.nz/cybersmart