THREE PILLARS | YOU ONLINE

stay on top of your security by protecting your three pillars, most forms of compromise start with one of them.

MAIN PASSWORD

EMAIL

DEVICE

CyberSmartKiwis

MAIN PASSWORD

your main password refers to your primary email password.

USE A LONG, UNIQUE PASSWORD

- **Length and uniqueness are your strongest defences.**

A long password is significantly harder to crack, and using a different one for each account prevents a single breach from unlocking everything else.

USE A PASSWORD MANAGER

- **Allows you to generate and store complex, unique passwords**

Without needing to remember them all, reducing the temptation to reuse or simplify passwords.

ENABLE MULTI-FACTOR AUTHENTICATION

- **Even if your password is compromised, MFA adds a critical second layer**

This makes it much harder for attackers to gain access.

FACT

A security audit uncovered that over 150 million records potentially connected to New Zealand were accessible on the dark web, containing thousands of active passwords - NCSC NZ

CyberSmartKiwis

EMAIL

your primary email address should be the most secure.

USE SEPARATE EMAIL ADDRESSES

- **For different purposes**

Keep a dedicated email for sensitive accounts (e.g. work, banking, health, education) and a different one for shopping or sign-ups, this limits exposure.

USE DISPOSABLE OR “BURNER” EMAILS

- **For one-off interactions**

When signing up for discounts, downloads, or unfamiliar sites, use a temporary email address. This protects your primary inbox from breaches. and there is many sites that provide a temp mail service for free.

SECURE YOUR PRIMARY EMAIL

- **Like a high-value account**

Use a strong, unique password and enable MFA. Since your main email controls password resets and account recovery, keeping it locked down prevents attackers from gaining wider access, change this password once a year.

FACT

Phishing and credential harvesting remain one of the top categories of cyber incidents reported in New Zealand, with emails being the primary target of this. - Internal Data

CyberSmartKiwis

DEVICE

your device is a digital copy of you and your life - protect it the same way.

UPDATE AND PROTECT YOUR DEVICE

- **Regularly install OS and app updates, use reputable security software**

Updates patch known vulnerabilities that attackers actively exploit, reducing the risk of malware or unauthorised access, including threats you can't see.

USE STRONG ACCESS CONTROLS

- **This prevents others from accessing your data if the device is lost,**

Set a PIN, password, or biometric lock, enable auto-lock, and encrypt your device if available.

BE CAUTIOUS WITH...

- **Downloads, apps, and connections**

Only install apps from official stores, review permissions, and avoid connecting to unsecured public Wi-Fi for sensitive activity. Many attacks rely on malicious apps or insecure networks to gain access to your device and data.

FACT

Malware can even be embedded in official apps, such as mobile games or QR code scanners - these app delay the malware deployment, then spam the device with adware after harvesting enough information from the device - Internal Data

CyberSmartKiwis