Cyber Security Guidance

National Cyber Security Centre

*The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Recipients can spread **TLP: CLEAR** information to the world, there is no limit on disclosure. Information sources may use **TLP: CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP: CLEAR** information may be shared without restriction.*

Guidance for high-profile individuals

What does 'high-profile' mean?

Individuals may become 'high profile' through the nature of their work and relationships.

For example, you may be considered a high-profile individual if you are:

- an elected central or local government representative;
- appointed to governance roles in major publicly traded companies or public sector organisations;
- an academic or advisor who has expertise in a field of geostrategic interest (e.g. strategic studies, international relations, or advanced research);
- a senior public servant with access to or influence over policy decisions, public expenditure, or information that impacts New Zealand's national security;
- a community leader or someone with a prominent role within a diaspora.

The list above is not exhaustive. If you are concerned that state actors might target you due to your role, influence or the activities you undertake, then the advice in this guidance is for you. Please follow it.

As a high-profile individual, your cyber security practices need to be more thorough than the average person's.

Secure yourself against common threats

Cyber threat actors can use a variety of methods to gain access to your accounts and devices; however, even basic protections can prevent some of the most sophisticated attacks.

There are many steps you can take to improve your personal cyber resilience. The advice included in this guide covers technical configurations and behavioural changes that can help you prevent

compromise. The advice in this section is also available separately as a condensed four-step action plan to help you start your journey.

Without adequate protection you may become an easier target for threat actors.

Identify your digital assets

A good first step is to create a list of your digital assets, including: hardware, software, online accounts, and any digital platform on which you store valuable information.

Creating a simple register, or list, will help you to easily identify the scope of your digital assets. By using our recommendations, you can mitigate your risks.

Have good password hygiene

Although this may be considered a basic measure, having long, strong, and unique passwords to protect your accounts is important. An easy way to create a good password is to make a passphrase made up of four or more random words. Passphrases are easier to remember, and they're stronger than a password that uses a long mix of numbers, letters, and symbols.

- Long: a minimum of 15 characters.
- Strong: use upper- and lower-case letters and, when required, a mix of numbers and special characters.
- Unique: do not repeat passwords, do not use a similar formula to create new passwords.

A **password manager** is a smart way to manage your passwords. It acts as a vault that stores all your device and account passwords in a secure, encrypted library. The only password you need to remember is the one that lets you access the password manager.

Password managers have many benefits, such as removing the need to remember all your complex passwords, providing the ability to create new, strong passwords, and providing a convenient single location to store them. Password managers can also be used to automatically fill in passwords to sign-in pages.

We strongly recommend that you do not use your web browser's 'remember password' feature because if an attacker were to exploit a vulnerability in your browser, it could serve as a gateway for cybercriminals to access your stored passwords.

Learn more about password managers, including how to choose one:

Keep your data safe with a password manager

https://www.ownyouronline.govt.nz/personal/get-protected/guides/keep-your-data-safe-with-a-password-manager/

Share accounts; do not share passwords

Sometimes you will need to share access to information or accounts. These shared accounts typically have administrator privileges and are used to manage a service. An example of shared access to information is using Microsoft Outlook to share your Outlook Calendar with specific individuals and restricting the level of detail they can see in your appointments.

Users with this shared access should be managed to ensure they:

- each have individual access with their own unique passwords;
- are vetted for security (depending on organisational policy); and
- are limited to only those who require access as part of their role.

When staff with access to shared information exit your organisation, ensure their account's access is disabled or removed, and use those actions as a prompt to change existing passwords.

Never share your passwords. Only you should know your passwords and have access to your password management tools in which your passwords are safely recorded.

Multi-factor authentication (MFA)

MFA, or multi-factor authentication, is also known as two-factor authentication or two-step verification. MFA is a tool that proves you are who you claim to be. 'Multi-factor' refers to needing more than one form of authentication to log in to an account or device.

MFA uses a combination of:

- something you know – such as your username and password;
- something you have – such as a security token, a device, or a unique code; and,
- something you are – such as your fingerprint or face ID.

MFA might be the most important security step you can take.

As a high-profile individual, we encourage using advanced MFA options that are more secure than SMS (text message) authentication. Examples of advanced MFA include physical tokens (such as YubiKeys, Google Titan keys, or FiDO2 keys) and passkeys. These forms of MFA are more secure because a threat actor would also require physical access to them to access your account, while text message codes could be phished or intercepted remotely.

If you receive an MFA request that asks if you are trying to access your account, but you have not attempted to log in, do not grant permission. It is possible that an attacker knows your password and is trying to access your account. In this instance, MFA is doing its job, but you should change your password. If you use the same password on other accounts, you should change the password for those accounts as well (and use your password manager to create unique passwords). Do not use the same password for multiple accounts.

MFA is an additional layer of security that creates extra barriers to prevent an attacker from accessing your information.

Regular updates and scanning

It is important to regularly update your devices with the latest software and firmware patches for security. We recommend enabling automatic updates for all your devices, so that updating happens conveniently, reliably, and consistently. This is especially important for all your device operating systems as well as home router firmware which will require you to enable and configure these updates in the devices settings.

Regular malware scanning is important to determine if your device has been infected. You can use the anti-malware programme built into your device, if there is one available. You should configure your device to scan new files automatically, and you should run a full system scan weekly.

We recommend scheduling weekly automated updates for your operating system and daily updates for anti-malware tools.

Set your devices to scan for malware whenever a file is opened, and conduct a full system scan every week.

We recommend that you consider anti-malware scanning for all your devices. Most routers come with a firewall that has pre-set rules for how it will manage your traffic. Enabling and configuring a firewall through device settings on your router will add an additional layer of security.

Social media

All social media accounts have privacy configuration settings. Take the time to understand how your online accounts appear to strangers and friends. This can typically be done using the 'view as' option.

Check that your privacy settings restrict how people can search for you on each platform, and limit who is able to send you private messages. As with emails and text messages, do not click on links sent to you via social media from people you do not know or trust. Do not click on unsolicited links to files in storage services such as Google Drive.

Limit the amount of personal information you share online and restrict access to that information to only the people you trust.

If you want to leave a social media platform, deactivate your account(s), but do not delete them – this means no one can take the username afterwards and pretend to be you. If you discover that someone is impersonating you online, immediately contact that platform's customer support and report it to us using the links below.

Learn more about social media safety guidelines:

Stay safe on social media

https://www.ownyouronline.govt.nz/personal/get-protected/guides/staying-safe-on-social-media/

Joining Wi-Fi at home and when away

At home:
Ensure your home network is protected with your own unique password, and that you have changed the default router name, which identifies the make and model. You should also change the default administrator password and username used to access the router administrator portal.

Learn more about securing your home network:

Secure your home network

https://www.ownyouronline.govt.nz/personal/get-protected/guides/secure-your-home-network/

Away from home:
Public Wi-Fi networks present a security risk because malicious users could intercept your network activity or attempt to access your devices without your knowledge.

Understand the risks of using free Wi-Fi networks in hotels, airports (including airline lounges), coffee shops, or other public spaces. If it's required, we recommend you use your mobile phone to hotspot. Always enable cellular data where possible when not connected to a trusted Wi-Fi network.

Ensure you understand your obligations and responsibilities to your organisation when connecting to Wi-Fi.

Your organisation may issue you with a device that which uses VPN (virtual private network) software to protect you online by encrypting your network activity and providing you with remote access to work resources. If this is the case, you should follow your organisational policies for working remotely.

External USB devices and public charging stations

Never plug a USB device such as a memory stick or hard drive into your computer if you do not know where it came from or if it is given to you by someone else. The same advice also applies to plugging a USB device into your work and personal devices, too.

When travelling, carefully consider where you plug in your phone or laptop to charge. Public USB charging stations may be compromised by cyber criminals and used to infect your device with malware or steal your data.

Either charge your device from a mains power plug or use your own portable power bank. Maintain physical control of your devices as much as practicable.

If you know you will need to charge your device in a public space and do not have access to your own power bank or a mains power outlet, we recommend you carry your own USB data blocker. USB data blockers are designed to prevent your data from being accessed through charging cables while connected to a USB hub.

General security advice

Your awareness of general cyber security practices will go a long way in keeping yourself cyber secure.

A. Malware Free Networks (MFN) is the NCSC's threat disruption service. MFN has been developed to help defend against malicious activity impacting a broad spectrum of users. You can test whether your ISP is protecting you from these threats by visiting the MFN page on the NCSC website. You may wish to consider asking your internet service provider whether they offer MFN or other threat mitigations as part of their service offering.
Read about Malware Free Networks

https://www.ncsc.govt.nz/services/malware-free-networks

B. Never click on links in unsolicited emails, texts, or social media messages.

C. Be aware of 'spear-phishing' attempts – threat actors will target you directly and pretend to be someone you know personally, usually asking for sensitive information or something urgent.

D. Check to see if any of your accounts or details have been compromised by using the website Have I Been Pwned. It is a well-known database that checks to see if your email has been caught up in any data breaches.
Have I Been Pwned

https://haveibeenpwned.com/

E. Be aware of the tactics used by threat actors and use the **SOUP** mnemonic to gauge behaviour:

Suspicious – Are they raising your suspicion by taking an overly active interest in who you are?

Ongoing – Are they frequently approaching you and furthering ongoing conversation themes?

Unusual – Are they asking unusual or specific questions seeking detailed information?

Persistent – Are they persistently asking you additional questions to divulge more information?

F. Ensure you are also aware of physical device security.

- Create password or passphrases to securely lock your device.
- Do not leave your devices unlocked where others might be able to gain access to them.
- Be aware of anyone who might be 'shoulder surfing' to see your passcodes or read sensitive information.
- Use 'Find my device' tracking services to find and remotely lock or wipe your device if necessary.
- Ensure all installed applications are up to date and create a habit of uninstalling applications you no longer require.
- If you are selling, replacing or giving away your phone, or even sending it in for repairs, it's good to back up any data you want to keep and then do a factory reset to erase and protect your personal data.
- [Apple users] Turn on 'lockdown mode' for your mobile devices.
  About Lockdown Mode - Apple Support

  https://support.apple.com/en-nz/105120

  Lockdown Mode is an optional, extreme protection that's designed for the very few individuals who, because of who they are or what they do, might be personally targeted by some of the most sophisticated digital threats. Whilst it reduces the functionality of phone, lockdown mode makes it harder for adversaries to exploit your device.
- [Android users] Ensure that you are using **Google Play Protect**.

  https://support.google.com/googleplay/answer/2812853?hl=en

  Google Play Protect is a security suite for Android that includes a malware scanner, Find My Phone, and Safe Browsing. It is built into the Android operating system and works automatically.

The NCSC can be contacted by email at: **info@ncsc.govt.nz**
We encourage you to contact us at any time if you require any further assistance or advice.