



Cyber Smart Week 2024 – Editorial Pack

We've put this copy together so you can easily lift and shift Cyber Smart Week official messaging for your channels.

Cyber Smart Week is here!

This Cyber Smart Week (21-27 October), we're supporting the National Cyber Security Centre (NCSC) by encouraging you all to own your online. There are some simple prevention measures that we can all take to make life much harder for cyber criminals.

The scary reality is that New Zealanders lose \$198m to scams each year.

Because people assume they'd not be stupid enough to fall for an online attack, many of us don't take simple actions to protect ourselves online. However, people aren't foolish, they're optimistic, busy, juggling, and eager to please... like we all can be.

We're all human, and our humanity is what can make us vulnerable to online attacks.

While these fraudsters play on our human nature, there are things every New Zealander can do to protect themselves online. But NCSC's latest results highlight that many of us don't do them:

- 43% use the same passwords for their online accounts
- 30% admit to not using strong passwords for their main online accounts
- 32% do not use two-factor authentication for their main online accounts

All of which leave us vulnerable for scammers to prey on our innate kindness as a way into our hearts... and bank accounts. It is through this 'generosity' that we're inadvertently 'donating' to scammers every year.

So, for this year's Cyber Smart Week, NCSC is launching *The Scamathon*.

The Scamathon shows scammers who are excitedly thanking us for our kind donation, a bit like the Telethon events from the 70's and 80's. It's a way of showing us all how sometimes our kindness is preyed upon to get us reaching into our wallets for more sinister motives.

The campaign encourages people to avoid 'donating' to scammers, by showing ways we can all help stop *The Scamathon* – in particular, by:

1. Having long, strong and unique passwords, and
2. Turning on two-factor authentication across your online accounts.

Find out more about Cyber Smart Week and *The Scamathon* at ownyouronline.govt.nz/scamathon

Two key actions to help you own your online

Here are some easy steps you can do to help stay secure and in control of all your things online:

1. Create long, strong and unique passwords.

Use a different password for each account and avoid using personal information, like your date of birth, in your password. Passphrases (random phrases of four or more words, for example *coffeecountsasameal* or *mapsshouldbesouthsideup*) make for the best passwords. They're easy to remember but hard for attackers to crack.



2. Turn on two-factor authentication (2FA)

2FA is an additional layer of security that helps to protect your online accounts. A common form of 2FA is a unique code sent to your phone or taken from an app that only you have access to. You can use it to authenticate who you are every time you log in. That way, even if an attacker gets your login details, they still won't get in. Start by setting up 2FA on your bank, email and social media accounts.



Other actions to protect yourself online

Activate auto updates on apps and devices

Updates aren't just about getting the latest features available on apps and devices; they also protect you from any weaknesses or vulnerabilities that have recently been discovered and that could let attackers in. The easiest way to do this is by going to settings and turning on automatic updates.



Set your social media settings to private

Make sure your social media privacy settings are switched over to 'Private' or 'Friends only'. This way, you can control who sees what information you share and who you're sharing it with.



Think before you click

Be wary of opening links and attachments in text messages, emails or on social media. These can be used by attackers to get hold of your personal details, or to install malware on your device. Even if you think the text might be legitimate, it's better to go to the organisation's website using another method. If something sounds too good to be true, it probably is!



Report it

If you, or someone you know, experiences an online security incident, report it to CERT NZ. They're here to help New Zealanders protect and recover from online security threats and incidents.



cert.govt.nz/report