

Cyber Smart Week 2024

21-27 October 2024

Supporter Pack Overview

Kia ora, thank you.

Thank you for signing up to be a supporter of Cyber Smart Week. We are thrilled with the number of organisations who are committed to helping New Zealanders and small to medium businesses be more secure online.

This document provides you with an overview of this year's campaign, what is included in your supporter pack, and a whole lot of activities you and your team can do throughout the week to improve your cyber security.

Please note that this material is embargoed, all material cannot be used until Cyber Smart Week (21-27 October 2024).

Contents.

- About Cyber Smart Week.
- Why does Cyber Smart Week matter?
- We need your help.
- This year's campaign.
- Ways to get involved.
- Campaign assets to use.

About Cyber Smart Week.

Cyber Smart Week is our annual campaign that focuses on encouraging New Zealanders to be more secure online. It is a time in the year to amplify the importance of cyber security and to encourage all New Zealanders and small to medium businesses (SMEs) to take protective actions.

Cyber Smart Week is targeted at all New Zealanders and small to medium businesses. Your participation in this year's campaign is vital in helping us reach millions of New Zealanders and empowering them with tools and resources to protect themselves online.

Traditionally, CERT NZ has run Cyber Smart Week. However, CERT NZ has recently been incorporated into the National Cyber Security Centre (NCSC) so you will see that this year's campaign comes from NCSC.

Why does Cyber Smart Week matter?

Online security plays an important role in all our lives but, for many, it is seen as something that's too technical, time consuming or inconsequential.

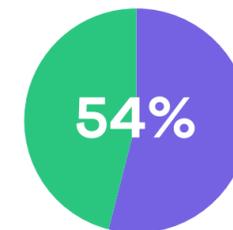
While no one will disagree that we are experiencing a rise in the number, and sophistication, of cyber attacks, many people underestimate the power they have in stopping these incidents in their tracks. It is up to all of us to take responsibility.

The effects of cybercrime are not just financial and reputational. It can also have a significant emotional impact on people and be extremely time consuming.

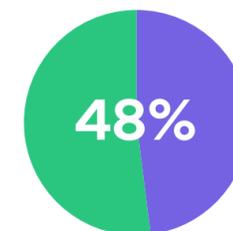
Last year's Cyber Smart Week campaign resulted in 70% of people who saw the campaign taking action to be more secure online. We want to use this year's Cyber Smart Week to continue to build a more resilient New Zealand.

\$198m lost to scams

(Oct 22-Sept 23*)



Over half of New Zealanders have experienced a cyber security event in the last 6 months.**



Less than half of small and medium businesses say they are prepared for a cyber incident.***

We need your help.

You play a massive role in helping New Zealanders to be more secure.

Our supporters play a critical role during Cyber Smart Week.

Your participation is vital in helping us reach millions of New Zealanders and empowering them with tools and resources to protect themselves online.

It is also a great opportunity to look at your own team's security and to use the week to amplify the importance of everyone taking personal responsibility.

All of this makes a big difference in helping build a more resilient New Zealand.

Cyber Smart Week 2024

This year's campaign.

// NCSC

own
your
online
cyber smart week

The problem.

Every year, New Zealanders lose \$198m to scammers and cyber criminals.

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 some simple prevention measures that every New Zealander can take to make life much harder for these criminals. But we don't always 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

The actions.

This Cyber Smart Week, we want to:

- Continue to raise the importance of being secure online
- Motivate New Zealanders and businesses to have the following protections in place



Strong password protections

Long, strong and unique passwords



Two-factor authentication (2FA)

Turn on 2FA across your online accounts

The idea.

Every year, scammers prey on our innate kindness as a way into our hearts... and bank accounts.

Through this 'generosity', we're inadvertently 'donating' \$198m to scammers every year.

So, this Cyber Smart Week, we're riffing off the ultimate donation mechanic – the Telethon.

Introducing: The Scamathon

The Scamathon shows scammers who are excitedly thanking us for our kind donation. Doing conga lines. Singing around a microphone. Live-Aid style. And sitting in tiered telethon-style seating wearing Madonna-mics as they 'take calls.'

All anonymously hidden behind a black bar covering their eyes.

It's an irreverent way to show 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 cyber criminals, by showing ways we can all stop supporting The Scamathon – by having long and unique passwords and turning on two-factor authentication.



Cyber Smart Week 2024

Ways to get involved.

// NCSC

own
your
online
cyber smart week

Ways to get involved.

Think

- Think about how you'd like to use Cyber Smart Week to help your organisation, employees and customers to be more secure online and more cyber resilient. An internal or external initiative – or both?
- Think about some key areas of focus:
 - Are there any cyber security actions that you'd like to see a shift with within your organisation? What needs to be done to make that change?
- Think about what additional opportunities, such as potential partnerships, might look like to further support and enhance your impact.

Plan

- How can you raise the importance of being secure online and get people to take action?
- How you are going to use the campaign assets in this supporter pack during Cyber Smart Week.
- Check out the suggested activities and tools on the following pages.
- How can you share the message externally to help keep your customers and suppliers safe and secure online?

Share

- Take photos of all your Cyber Smart Week events and activities.
- Share and tag us in your posts
Facebook: [@ownyouronline](#)
Instagram: [@ownyouronline](#)
LinkedIn: [@cert nz](#)
We'll help promote!
- Use our official Cyber Smart Week hashtags:
[#CSW24](#)
[#StopTheScamathon](#)
[#OwnYourOnline](#)
This will help us see it all!
- Link to:
ownyouronline.govt.nz/scamathon
(this page will go live by 21 October)

Scamathon challenge.

Cyber Smart Week is the time to bring your team up to speed on cyber security. Here's some challenges to complete during the week:

Introduce the week

Present to your team: use our short PowerPoint presentation (included within this supporter pack) to provide your team with an overview of Cyber Smart Week and the actions you want your team to take.

Password challenge

Encourage your team to review the passwords on their main accounts, such as email, banking, social media and key business logins.

Make sure they are long, strong and unique.

[Create good passwords - Own Your Online](#)

2FA challenge

Get your team to enable two-factor authentication on a different account every day for a week. Have them start with their email, bank and social media accounts, along with key business accounts.

Our 2FA webpage will be updated in time for Cyber Smart Week to give you links that step you through how to do this for your main bank, social and email accounts.

[Use two-factor authentication to protect your accounts - Own Your Online](#)

Watch our business training videos as a team and discuss

Our new Unmasked Cyber Crime training videos will be available mid-October. They are an easy guide to the cyber security practices you need to consider for your organisation.

We will email you when these are available.

Scamathon challenge.

Cyber Smart Week is the time to bring your team up to speed on cyber security. Here's some challenges to complete during the week:

Take one of our quick and easy self-assessment tools

Answer a few questions about your online security behaviour and habits to get a customised action plan to help you and your business become more secure online.

- Personal online security assessment tool:
[Online security assessment tool - Own Your Online](#)
- Business online security assessment tool:
[Business online security assessment tool - Own Your Online](#)

Sign up to a Cyber Smart Week webinar

We will be running a series of webinars throughout Cyber Smart Week. These will be tailored for specific sectors, including finance, SME, consumer, tech, health, government and advisors. We will email you separately with instructions on how to register for these.

Incident planning

What would happen if your organisation had a serious cyber security incident?

Check out our Incident Response Plan template on ownyouronline.govt.nz/business and fill it in.

Quiz and word find

Try our Own Your Online quiz and/or word find in this supporter pack.

Cyber Smart Week 2024

Campaign assets to use.

// NCSC

own
your
online
cyber smart week

What's included.

Your supporter pack contains all the material you can use to share the campaign on your channels throughout the week.

Below is an overview of all the assets available in your pack:

- Terms & Conditions
- Editorial pack
- Website pack
- Social media pack
- Posters
- EDM banners
- Screensavers
- Quiz and word find
- PowerPoint presentation
- Translated content

Important notes:

The campaign URL to direct people to for more information is ownyouronline.govt.nz/scamathon

If you would like to create your own material and would like to use the Cyber Smart Week lockup, please email us at cybersmart@ncsc.govt.nz

We are currently in the process of having some key campaign assets translated into te reo Māori. If you would like to receive these when available, please email us cybersmart@ncsc.govt.nz

This material is embargoed, and all material cannot be used until Cyber Smart Week (21-27 October 2024).

Editorial pack.

In the editorial section of your supporter pack, you'll find copy and images that you can easily lift and shift for emails, newsletters and articles you write.



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

// NCSC



Key actions to help you own your online

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

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 *coffeeaccountsasameal* or *mapsshouldbesouthsideup*) make for the best passwords. They're easy to remember but hard for attackers to crack.



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.



Actions to protect yourself online

Keep updates on apps and devices

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



Set social media settings to private

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



Don't click

Be careful not to click on 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 spy on your device. Even if you think the text might be legitimate, it's always best to go to the organisation's website using another method. If something seems too good to be true, it probably is!



If someone you know, experiences an online security incident, contact the National Cyber Security Centre (NCSC) or CERT NZ. They're here to help New Zealanders protect and respond to online security threats and incidents.



ownyouronline.govt.nz/report



Website pack.

Where possible on your website, we recommend that these tiles direct people to ownyouronline.govt.nz/scamathon to find out more information.

You can use the copy in the Editorial Pack alongside these tiles.

Scamathon creative:

Introduction to
Cyber Smart Week:

2FA:

Passwords:



Own Your Online/Generic creative:

2FA:

Passwords:



Social media pack.

In the social media pack, we have given you recommended wording and images that you can use in your social posts and stories throughout Cyber Smart Week. This includes:

- Copy and images that you can use
- Two different creative options to choose from: The Scamathon and Own Your Online/Generic
- 1080x1350 and 1080x1920 image formats for both in-feed and story content
- Details on the hashtags and accounts to tag and follow

Scamathon creative:

Introduction to
Cyber Smart Week:



2FA:



Passwords:



Own Your Online/Generic creative:

2FA:



Passwords:



Posters.

These can be printed out in colour or black and white, at A4 or A3.

Scamathon creative:

Introduction to
Cyber Smart Week:

2FA:

Passwords:



Own Your Online/Generic creative:

2FA:

Passwords:



EDM banners.

Scamathon creative:



Own Your Online/Generic creative:



Screensavers.

Scamathon creative:



Own Your Online/Generic creative:



Translated content.

As part of our Own Your Online resources, you also have available a suite of translated copy and short-form videos.

These assets are to help people who don't speak English as a first language understand the importance of two-factor authentication and long, strong and unique passwords. The content is available in Tongan, Samoan, Cook Island Māori, Fijian, Korean, Punjabi, Chinese, and Hindi.

Translations about 2FA & Passwords: (including videos)

온라인 보안 유지

Korean:

[Korean - keeping secure online - Own Your Online](#)

ऑनलाइन सुरक्षित रहना

Hindi:

[Hindi - keeping secure online - Own Your Online](#)

ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣਾ

Punjabi:

[Punjabi - keeping secure online - Own Your Online](#)

Tausisia saogalemu i luga o le initaneti

Samoan:

[Samoan - keeping secure online - Own Your Online](#)

确保上网安全

Simplified Chinese:

[Simplified Chinese - keeping secure online - Own Your Online](#)

Tauhi 'a e malu 'i he 'initaneti

Tongan:

[Tongan - Keeping secure online - Own Your Online](#)

Mo qaqarauni ena initaneti

Fijian:

[Fijian - keeping secure online - Own Your Online](#)

Te turanga ponuiā'au i runga i te 'ātuitui roro uira

Cook Island Māori:

[Cook Island Māori - keeping secure online - Own Your Online](#)

(without video)

Ētahi huatau pai mō te haumarū ā-ipurangi

Te reo Māori:

[Te reo Māori - keeping secure online - Own Your Online](#)

關於網路安全的重要提醒

Northern Chinese:

[Northern Chinese - Own Your Online](#)

Alternative Resources

More resources in alternate formats can be found [here](#).

We are currently in the process of having some key campaign assets translated into te reo Māori. If you would like to receive these when available, please email us cybersmart@ncsc.govt.nz

Thank you

for contributing to keeping New Zealanders safe online.

If you have any questions about getting involved with Cyber Smart Week, please reach out to us.

We're happy to help, email us at cybersmart@ncsc.govt.nz