

own
your
online

Cyber Smart Week 2025

Explaining your Supporters Pack

NCSC

Kia ora, thanks for supporting Cyber Smart Week

Online security is increasingly important for New Zealanders and businesses. During Cyber Smart Week we want to raise the importance of being secure online, but we can't do it alone. Your support makes a significant difference in encouraging more New Zealanders to take action to better protect themselves.

In this document, you'll find an overview of this year's campaign, what's included in your supporter pack, along with activities you and your team can do throughout the week.

Please note that all materials in this pack are embargoed until Cyber Smart Week (6–12 October 2025).

Contents

About Cyber Smart Week	04
We need your help	05
Why does Cyber Smart Week matter?	06
This year's campaign for supporters	07
Ways to get involved	13
Campaign assets to use	21

About Cyber Smart Week

What: Cyber Smart Week is our annual campaign that focuses on the importance of being secure online. It's a week of activity that encourages all New Zealanders to take simple yet effective steps to protect their online lives.

When: Monday 6 October – Sunday 12 October

Who: Online security affects all of us, and touches many aspects of each of our lives. So this week is important for all New Zealanders, organisations and community groups.

Cyber Smart Week is coordinated by the **National Cyber Security Centre (NCSC)**, using our **Own Your Online** sub-brand.

Please note that all materials in this pack are embargoed until Cyber Smart Week (6 – 12 October 2025).

We need your help

You play a massive role in helping your employees, customers, stakeholders and communities to be more secure online.

It is also a great opportunity to look at your own team's security and take proactive steps to minimise your exposure.

Together, let's build a more resilient New Zealand.

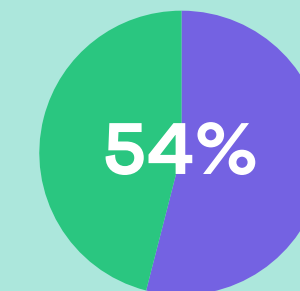
Why does Cyber Smart Week matter?

New Zealanders lose a massive \$1.6 billion per year to online security threats. On average, that's \$1,950 lost per person. Yet our research tells us that only 42% of New Zealanders feel vulnerable to cyber attacks.

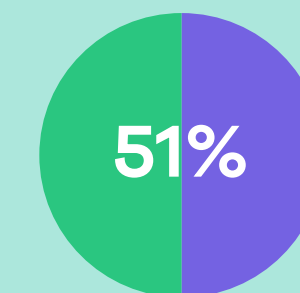
This level of misplaced apathy and confidence is leaving us all susceptible to losing our hard-earned cash. Creating stress, anxiety and lost time and money for many New Zealanders.

Everyone has a role to play in protecting New Zealanders and businesses online – government, businesses, communities, individuals – and Cyber Smart Week is a great opportunity to remind us all to take some simple yet effective actions that can help to stop cyber criminals in their tracks.

\$1.6B
lost to scams



Over half of New Zealanders have experienced a cyber security threat in the last six months.



Half of all small to medium sized businesses admit to not feeling prepared when it comes to preventing a cyber security breach.



Cyber Smart Week 2025

This year's campaign for supporters

**own
your
online**
cyber smart week

Take a moment to own it

This year we're encouraging everyone to **take a moment to own it** with some simple steps to help protect yourself, your team and your community online.

And it can be easier than you think:



1. Use long and unique passwords

Because we know 46% of people admit to using the same passwords across multiple accounts.



2. Turn on two-factor authentication

Because 32% of people admit to still not using 2FA on their main accounts.

In particular, we're encouraging New Zealanders and businesses to start with their main accounts: **banking**, **email** and **social media**. This will have the biggest immediate impact at keeping yourself secure.

Key stats for you to use

Here are some key stats that you may find useful to use in your comms:

General size of the problem:

No one is immune from being targeted by cyber crime

Yet:

Only 42%

of New Zealanders feel personally vulnerable to cyber attacks online*

54%

of New Zealanders have experienced an online security attack in the last six months*

\$1.6 billion

New Zealanders lose (conservatively) each year due to online threats. On average, that's \$1,950 lost per person*

That's because people often think:

"It's not worth prioritising"

"It won't happen to me"

"It's too time consuming"

*Cyber Security Behaviour Tracker 2025, NCSC, May 2025 (Report link: [cyber-security-behaviour-tracker-2025.pdf](#))

Key stats for you to use

Here are some key stats that you may find useful to use in your comms:

Passwords:

A long, unique password (with 16+ characters) can take billions of years to crack.

Yet:

46%

of New Zealanders admit to using the same passwords online*

Two-factor authentication:

Two-factor authentication helps to stop 99% of automated online attacks.

Yet:

32%

of New Zealanders admit to not using two-factor authentication on their most important accounts (bank, email, social media)*

*Cyber Security Behaviour Tracker 2025, NCSC, May 2025 (Report link: [cyber-security-behaviour-tracker-2025.pdf](#))

Key stats for you to use

Here are some key stats that you may find useful to use in your comms:

Small to medium businesses:

Half of all small to medium sized businesses do not feel prepared when it comes to preventing a cyber security breach.**

Yet:

31%

don't use different passwords for their accounts**

1 in 4 (23%)

of businesses admit they don't use two-factor authentication**

30%

of small to medium businesses do not regularly back up their data and files**

**SME Cyber Security Behaviour Tracker 2025, NCSC (report available at ncsc.govt.nz from September 2025)

What are we doing?

How Exposed Am I?

Own Your Online is also launching a nationwide campaign during Cyber Smart Week, designed to show New Zealanders how we are all vulnerable to scammers and to encourage people to take action.

Called '**How Exposed Am I?**', the campaign launches on 6 October and includes:

1. An advertising campaign that prompts New Zealanders to reconsider how **vulnerable** they are, and directs them to an immersive web experience.
2. The immersive web experience, where you can discover what **personal information** has been **exposed** to scammers.

The purpose of this campaign is to break the **apathy** many New Zealanders have towards their online security by showing them how exposed they are. It works hand-in-hand with the 'Take a moment to own it' theme in this year's supporter pack.

Keep an eye out during Cyber Smart Week and learn how exposed your personal data could be. **It might surprise you.**



Cyber Smart Week 2025

Ways to get involved

**own
your
online**
cyber smart week

Ways to get involved

There are many ways to get involved and be a part of this year's Cyber Smart Week.

Below are some thought-starters for how you could look to engage your business, team or community in ways that are right for them. It's all about getting people to **take a moment to own it**, to help everyone get more secure online.

THINK IT

Think about what you or your team would like to have achieved by the end of Cyber Smart Week.

What is the shift you need to make to help your organisation be more secure online?

Think about some key areas of focus:

Are there any cyber security actions that you'd like to prioritise? What needs to be done to put that into action?

Think about if you're prepared for when something goes wrong:

Do your employees know what to do if they receive a phishing email, receive a random text pop up asking for money or to prevent a data breach?

Think about the best way to reach your employees or audience:

This could be online, in person, or via the community.

Think about what needs to happen to help people take action:

Have an approved password policy and password manager to make life simpler for your team.

PLAN IT

How can you raise the importance of being secure online and get people to take action?

Take a look through the campaign assets below:

How could you use and leverage these materials?
Could you make your own instead?

Organise your activity:

Organise an event, run a webinar, write a blog, create a quiz – let us know if you'd like us to help share it.

Make the most of it:

Plan your messaging, implement the changes you need to make and build momentum – think notice boards, social media, intranet, eDMs.

Rally the team:

What additional opportunities (like partnerships or collabs) are there that could help enhance your impact or further support you?

ENGAGE IT

Here are some ways you can engage your audience:

Tag, share and engage with us on social media:

LI: <https://www.linkedin.com/company/ownyouronline/>

FB: <https://www.facebook.com/ownyouronline>

IG: <https://www.instagram.com/ownyouronline>

Look at the activity ideas and challenges in this pack:

We have lots of ideas on how you can help your employees take a moment to own it.

Visit, share and engage with our campaign pages (live from 6 Oct):

ownyouronline.govt.nz/takeamomenttoownit

HowExposedAml.co.nz

Add your logo into our posters

Request the Own Your Online/Cyber Smart Week lockup

Take lots of photos of all your activities: We can help share!

Sign up to Own Your Online's newsletters:

[Subscribe - Own Your Online](#)

Activity ideas for your team

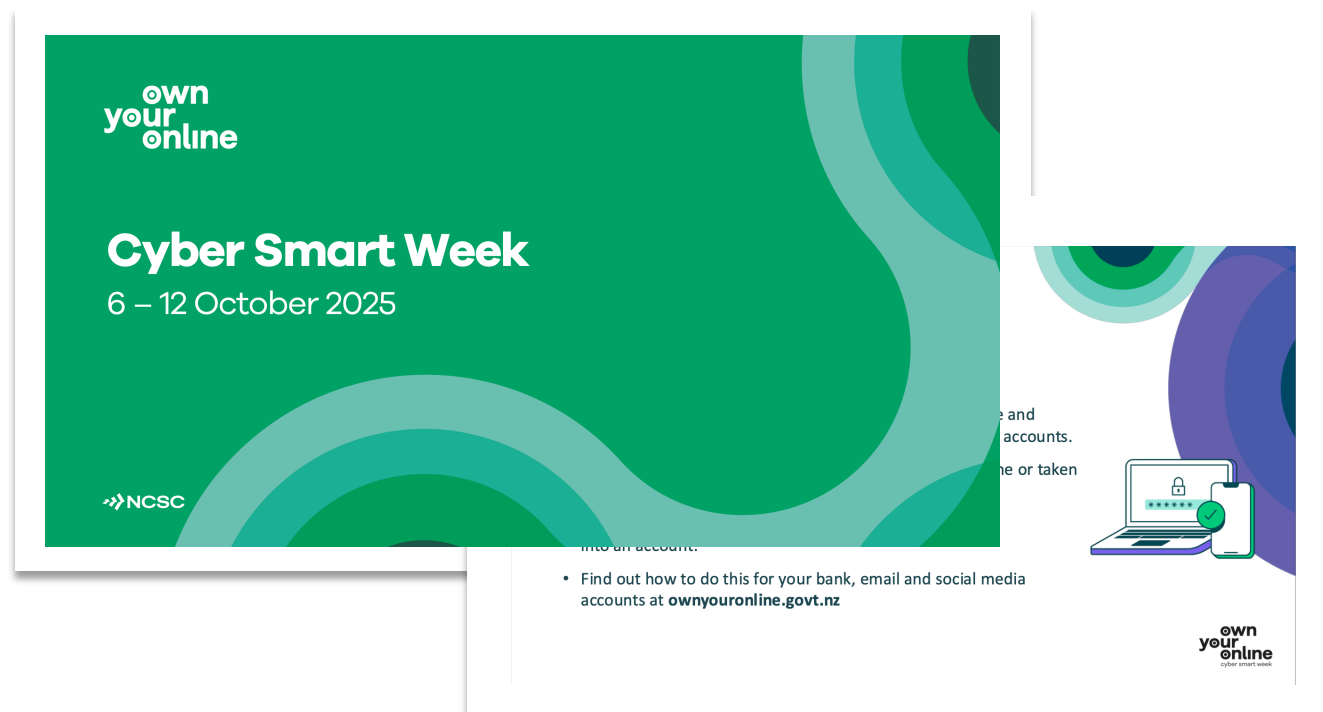
Here are some ideas to help encourage everyone to take a moment to own it – both at work and at home:

Introduce the week:

Present to your team with our short PowerPoint presentation (included in this supporter pack) to give them an overview of Cyber Smart Week and the key actions you want them to take.

Passblot challenge – What do you see?

In this pack, you'll find a series of 'inkblot' posters that challenge your team to create a strong passphrase from whatever they see in them. It's a fun way to create a unique, long password – put them up around your space, and challenge people to think differently.



Activity ideas for your team

Password challenge – How Exposed Am I?

On Monday 6 October, we'll be launching an immersive web experience where everyone can see how exposed they might be.

The results will be surprising for many, and is a great personalised demonstration of why online protections are so important.

HowExposedAml.co.nz

2FA challenge

Does everyone in your team have two-factor authentication enabled on their main online accounts? i.e. bank, email and social media accounts, and key business-critical online accounts.

2FA helps to stop cyber criminals access your accounts without your permission, so this is an important step to stay secure.

Our 2FA page gives you links that step you through how to do this for your main bank, social media, email and myIR accounts: [Set up two-factor authentication \(2FA\) - Own Your Online](#)

Activity ideas for your team

Attend a free webinar:

We'll be running a series of webinars throughout the week, with each webinar tailored to a different audience. See **Pg.20** for more detail.

Share the message:

Help spread the message by downloading our posters and redecorating your walls, utilising the editorial or making use of the other digital assets in this pack.

Take our quick & easy online quiz:

It's a fun way to assess your cyber security habits; just answer a few simple questions and you'll get a customised action plan to help you better protect yourself online.

[Online Security Assessment](#)

Make a game out of it:

Try our Own Your Online word find and bingo in this supporter pack.

Do you know how to spot phishing?

Watch our short video to learn what phishing is, how it works and how to protect against it:

Watch Now: [What is phishing?](#)

Activity ideas for your business

If you're a small business or community group that doesn't have a dedicated person looking after your security, here are some great ways to take a moment to own it:

Explore our Business Online Security Series

Watch our entertaining series of short videos, where we break down the cyber security basics for you and show what free and simple protections you can put in place now to get you started on securing your business.

Watch Now

[Unmask Cyber Crime – Own Your Online](#)



Activity ideas for your business

Take our online assessment tool

Grab a cuppa and take 5-10 minutes out of your day to learn how secure your business is and what you can do to level up.

[Give it a go.](#)

Attend our free webinar

"Cybercrime isn't personal, it's profitable: why small businesses are prime targets" **See Pg. 20.**

Create a password policy for your employees, using our template:

[Password Policy Template](#)

Prepare an Incident Response Plan, using our template:

What would happen if your business had a cyber security incident? Fill in our Incident Response Plan template now and be prepared:

[Incident Response Plan Template](#)

Free Webinar Schedule

We'll be running a series of webinars throughout the week. Please feel free to share this and [register here](#).

<p>Cybercrime isn't personal, it's profitable: why small businesses are prime targets</p> <p>Cyber security is no longer a "nice to have" for small businesses, it's essential. But that doesn't mean it has to be complicated or expensive.</p>	<p>Webinar for IT Security Specialists</p> <p>Cyber security is evolving faster than ever – and so are the threats.</p> <p>For IT professionals, security specialists, and those working on the frontlines of digital defence, staying ahead means understanding not just <i>what</i> is happening, but <i>how</i> it's happening.</p>	<p>Cyber security basics for individuals</p> <p>Staying safe online doesn't have to mean learning complex tech jargon or locking down your devices like a bank vault. A few small, smart changes can make a big difference.</p>	<p>Staying Safe Online – Older Online</p> <p>Being online is part of everyday life, whether it's keeping in touch with loved ones, doing banking online, or booking a GP appointment.</p> <p>In this practical webinar, we'll walk through everyday situations people might face online — and how to handle them with confidence.</p>	<p>AI, deepfakes and cyber threats</p> <p>Artificial intelligence is moving fast, and it's changing the threat landscape just as quickly.</p> <p>From deepfakes and voice cloning to AI-generated phishing emails, cyber criminals are already using these tools to deceive, manipulate, and exploit.</p>	<p>Education and Health: Protecting data and building trust</p> <p>Education and healthcare organisations hold some of the most sensitive and valuable information – student records, medical histories, personal details – and with that comes a growing responsibility to protect it.</p>
<p>Monday 6 October: 10:00 am – 11:00 am</p>	<p>Monday 6 October: 1:00pm – 2:00pm</p>	<p>Tuesday 7 October: 10:00 am – 11:00 am</p>	<p>Wednesday 8 October: 11:00 am – 12:00 pm</p>	<p>Wednesday 8 October: 1:00 pm – 2:00pm</p>	<p>Thursday 9 October: 10:00 am – 11:00 am.</p>
<p>Suited to: small businesses who do not have a dedicated person looking after their IT.</p>	<p>Suited to: People that have a technical cyber security background.</p>	<p>Suited to: Anyone wanting to learn where to start with cyber security, what the current biggest threats are and how to stay safe online.</p>	<p>Suited to: Older adults who use the internet for everyday things and want to feel more confident. You don't need any tech knowledge.</p>	<p>Suited to: Anyone who wants to learn about AI and what the implications on cyber security are – consumer and business.</p>	<p>Suited to: Those who work in environments that handle sensitive information, focus on healthcare and education, and anyone who handles confidential information.</p>



Cyber Smart Week 2025

Campaign assets to use

own
your
online
cyber smart week

Campaign assets to use

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

Here's an overview of all the assets available in your pack:

- Terms & conditions
- Editorial pack
- Website pack
- Social media pack
- Posters
- Screensavers
- Bingo & word find
- PowerPoint presentation
- Te reo Māori pack
- Translated content

Please note that all materials in this pack are embargoed until Cyber Smart Week (6–12 October 2025).

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

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

Editorial Pack

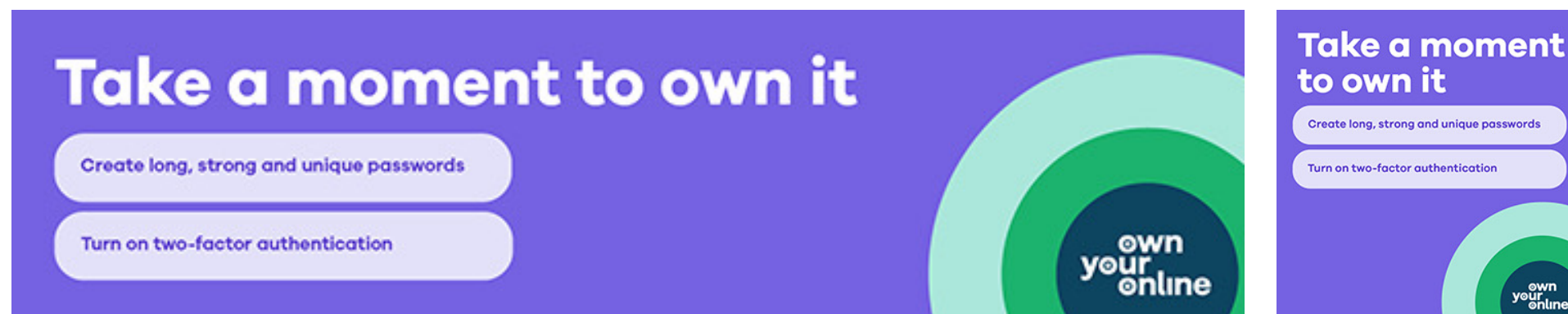
In the editorial section of your supporter pack, you'll find copy and images that you can easily lift and shift into articles, newsletters and emails you write.



Website Pack

Where possible on your website and intranet, we recommend that these banners and tiles direct people to **ownyouronline.govt.nz/takeamomenttoownit**

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



Social Media Pack

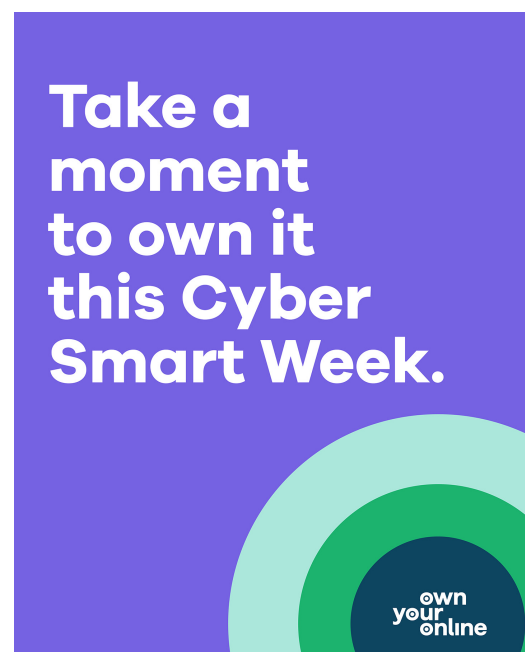
In the social media pack, we have given you recommended wording and images that you can use in your social posts and stories throughout Cyber Smart Week.

This includes:

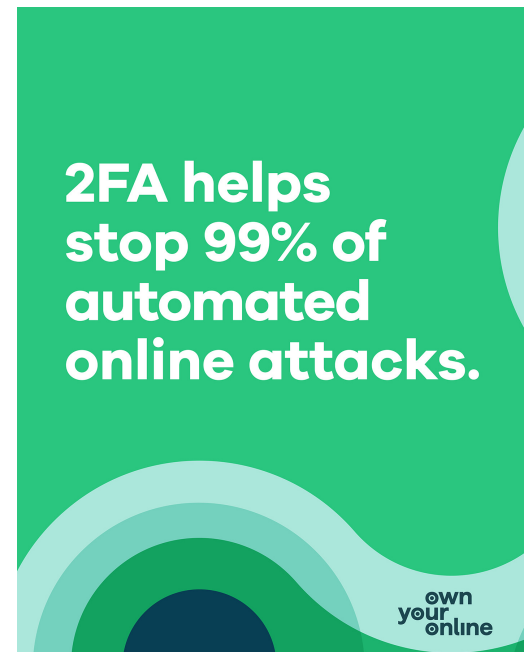
- Copy and images that you can use
- 1080x1350 images for in-feed content (FB, IG, LI)
- 1080x1920 images for story content
- Details on how to tag Own Your Online, and follow us

Take a moment to own it creative:

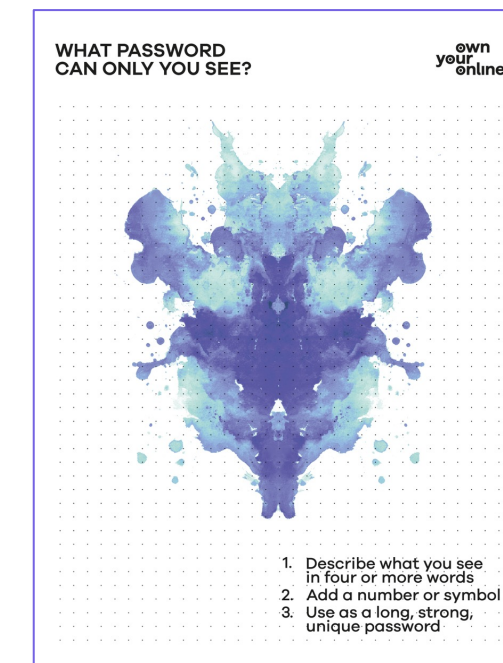
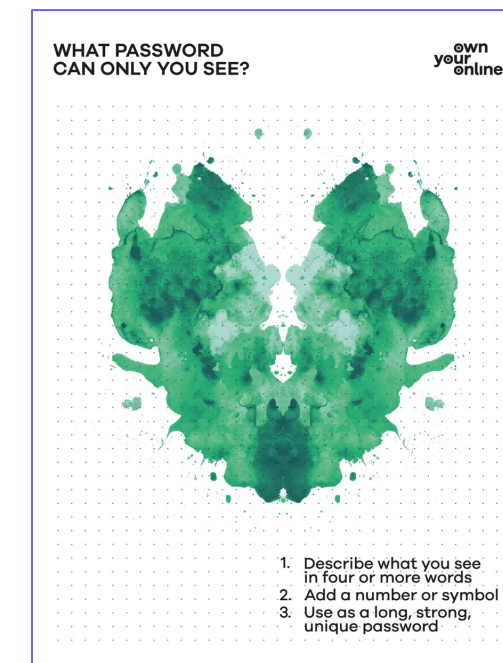
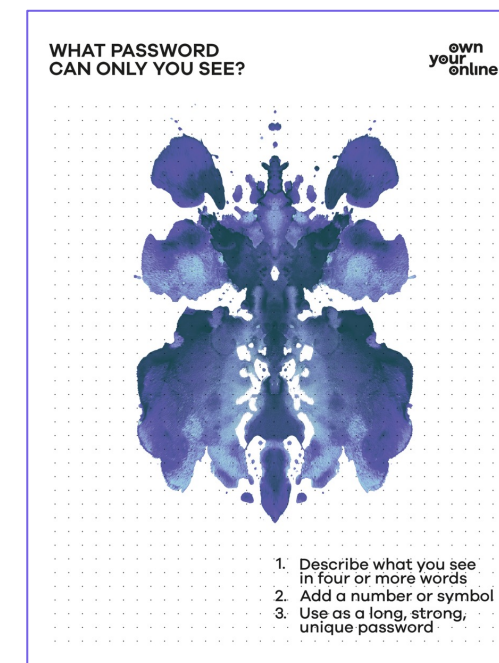
Take a moment to own it: Passwords:



2FA:



Passblots creative:



Posters

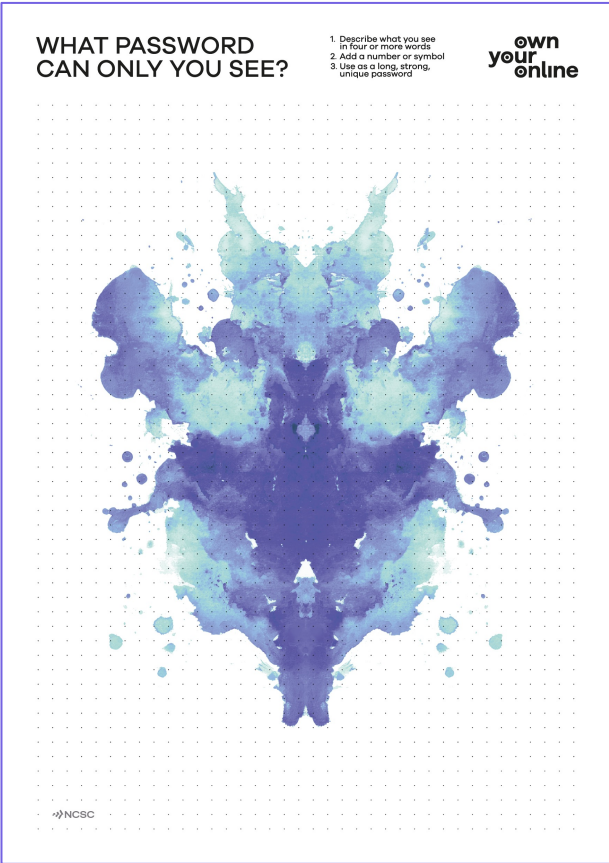
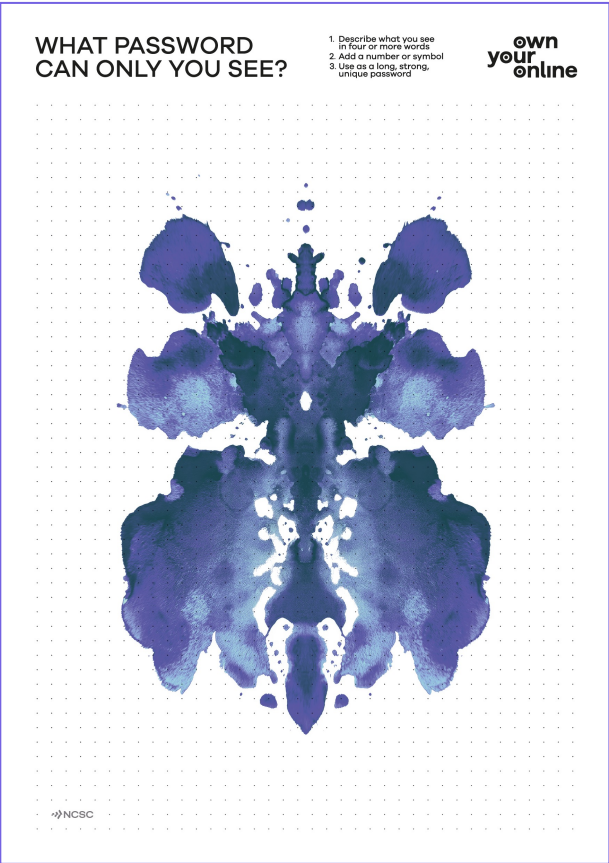
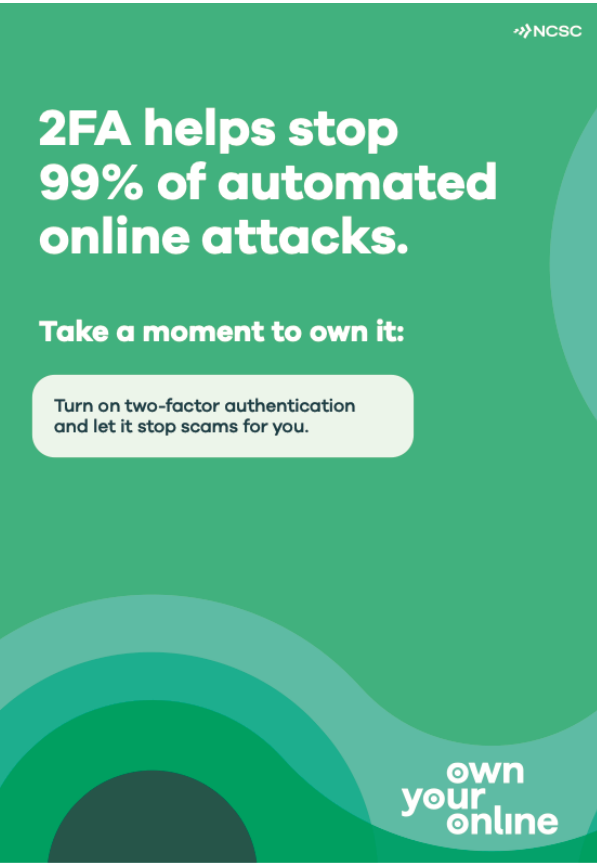
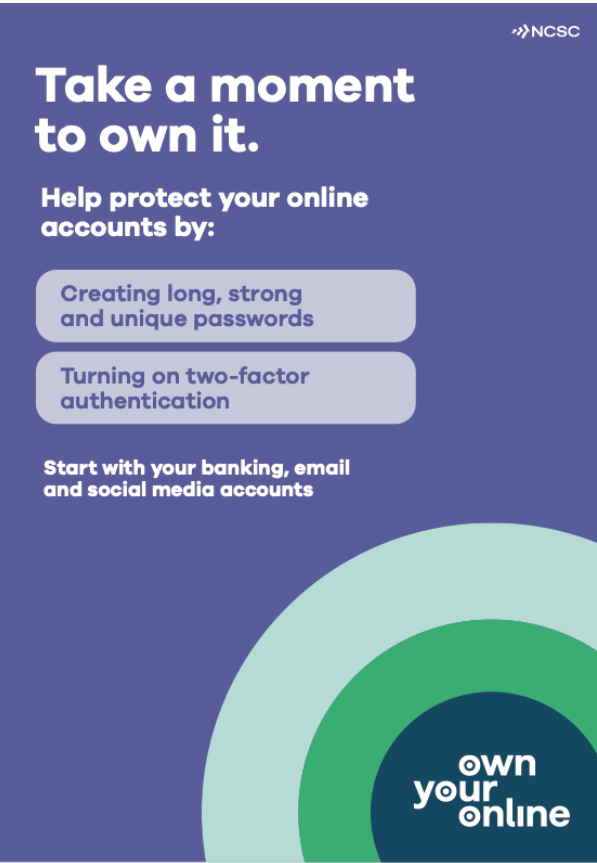
These can be printed out at A4 or A3. Colour printing is recommended where possible.

Take a moment to own it creative:

Take a moment to own it:

Passwords:

2FA:



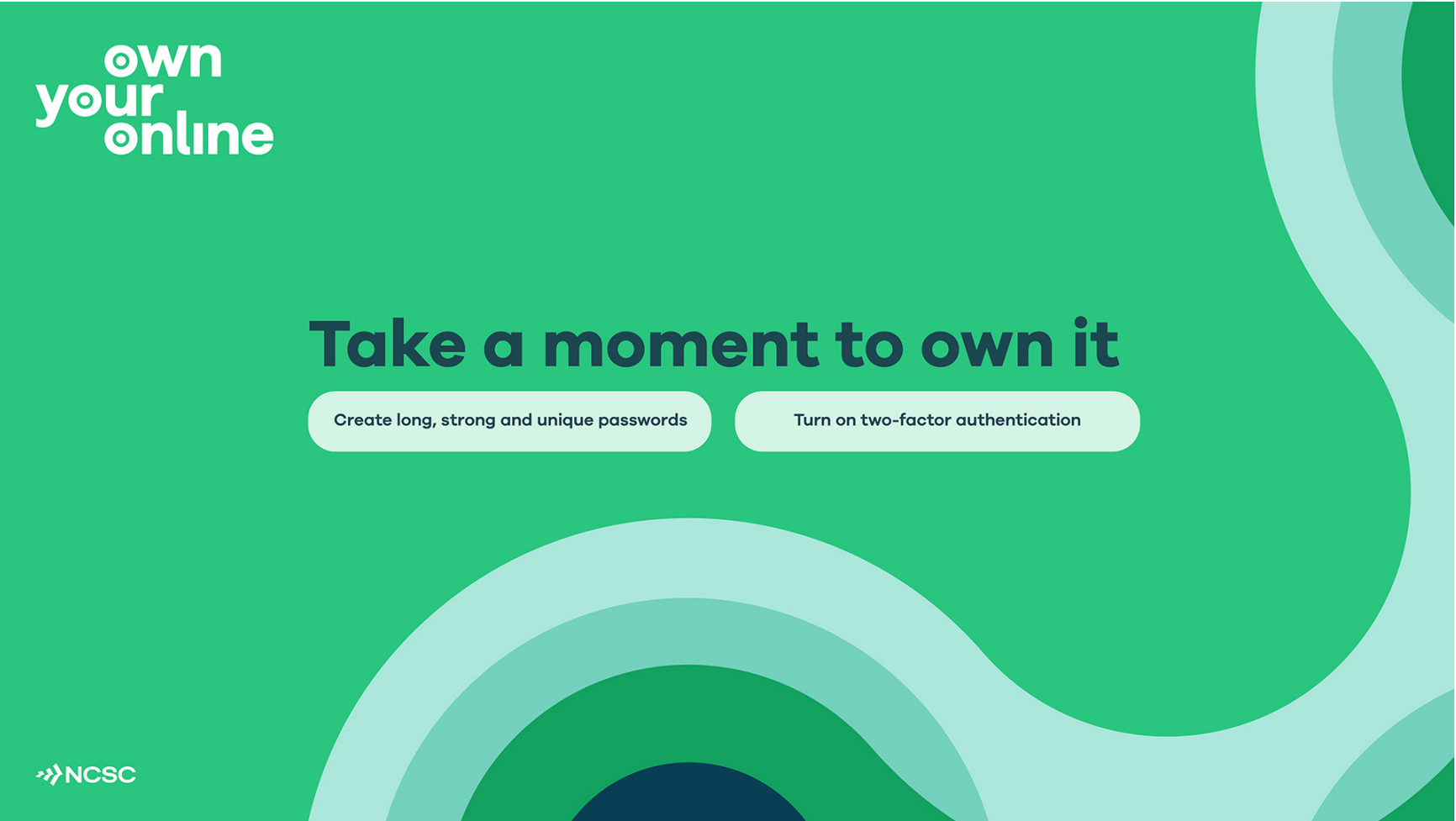
Adding your logo

- 1. Open Adobe Acrobat:** Launch Adobe Acrobat on your computer.
- 2. Open the PDF file:** Click on 'File' in the menu bar and select 'Open.' Locate and select the 'Add Your Own Logo' Poster PDF that you want to edit. You will find this in the 'Customisable Posters' folder, in your Posters folder.
- 3. Access the Edit tool:** In the right-hand panel, click on the 'Edit PDF' tool. This will enable the editing features of Adobe Acrobat.
- 4. Select the logo area:** Place your logo into the allocated space. You can see suggested allocations, in the examples provided to the right.
- 5. Insert your logo:** After selecting the area, right click within the selection and choose 'Add Image.' A file browser window will appear.
- 6. Locate your logo file:** Select the file. Insert it to the allocated spacing. If your business logo has a colour range please use dark tones on the light teal, and light tones on the purple or green. You can see this in the examples provided.
- 7. Adjust the logo position and size:** Reposition your logo, to the top right corner, and resize it to match the allocated space. Please ensure the sizing leaves enough clear space and does not encroach on the copy. Click on the logo to display resizing handles, then click and drag the handles to adjust the size. To move the logo, click and drag it to the desired location within the selected area.
- 8. Save the Changes:** To save the edited PDF document, click on 'File' in the menu bar and select 'Save' or 'Save As' to save the modified PDF document with your edits.

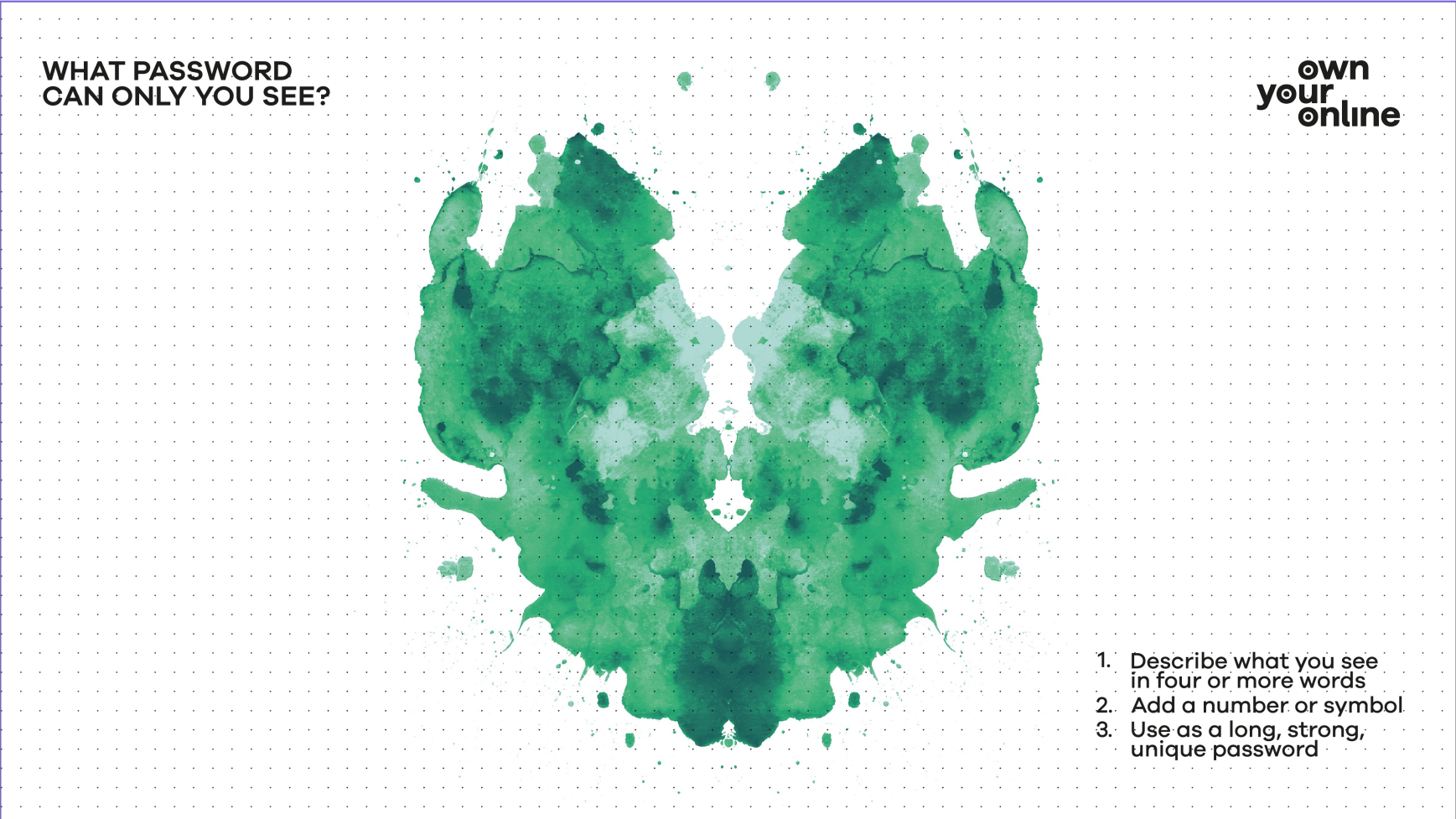


Screensavers

Take a moment to own it creative:



Passblots creative:



Te reo Māori pack

This pack includes:

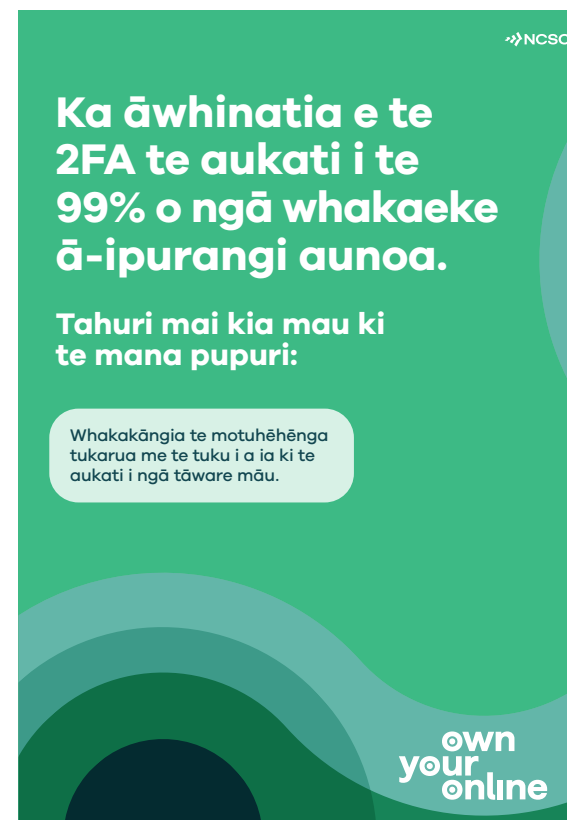
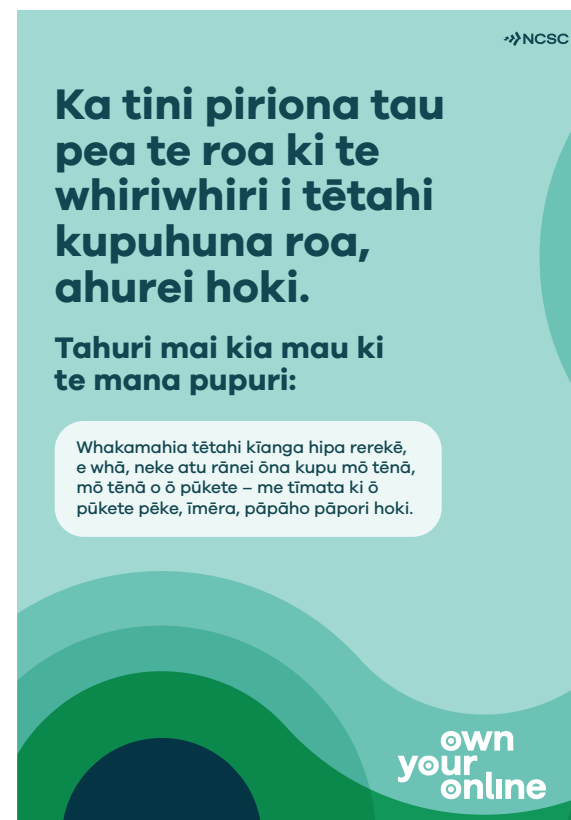
- Editorial copy
- Posters
- A social media post

Posters:

Take a moment to own it:

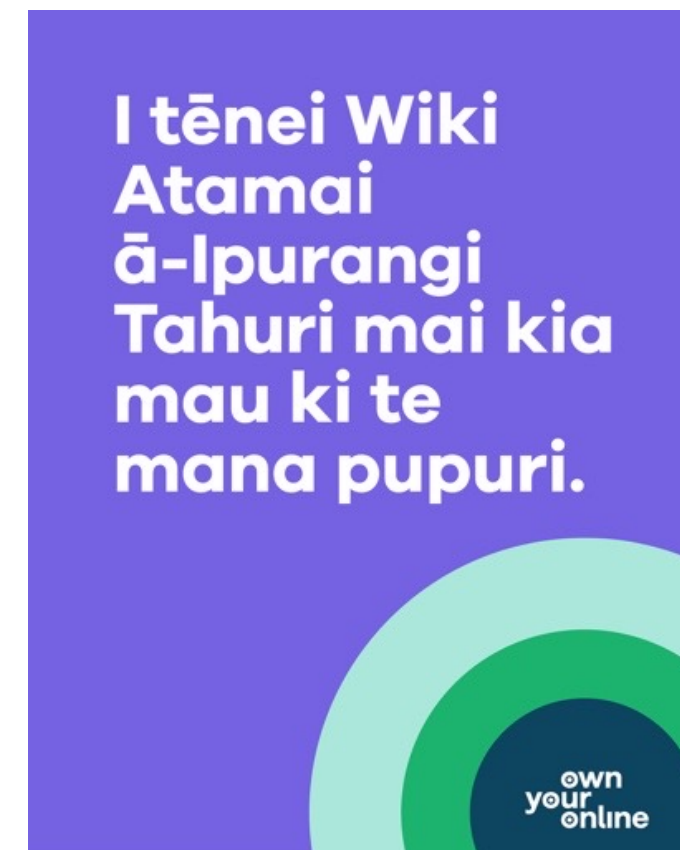
Passwords:

2FA:



Social Assets:

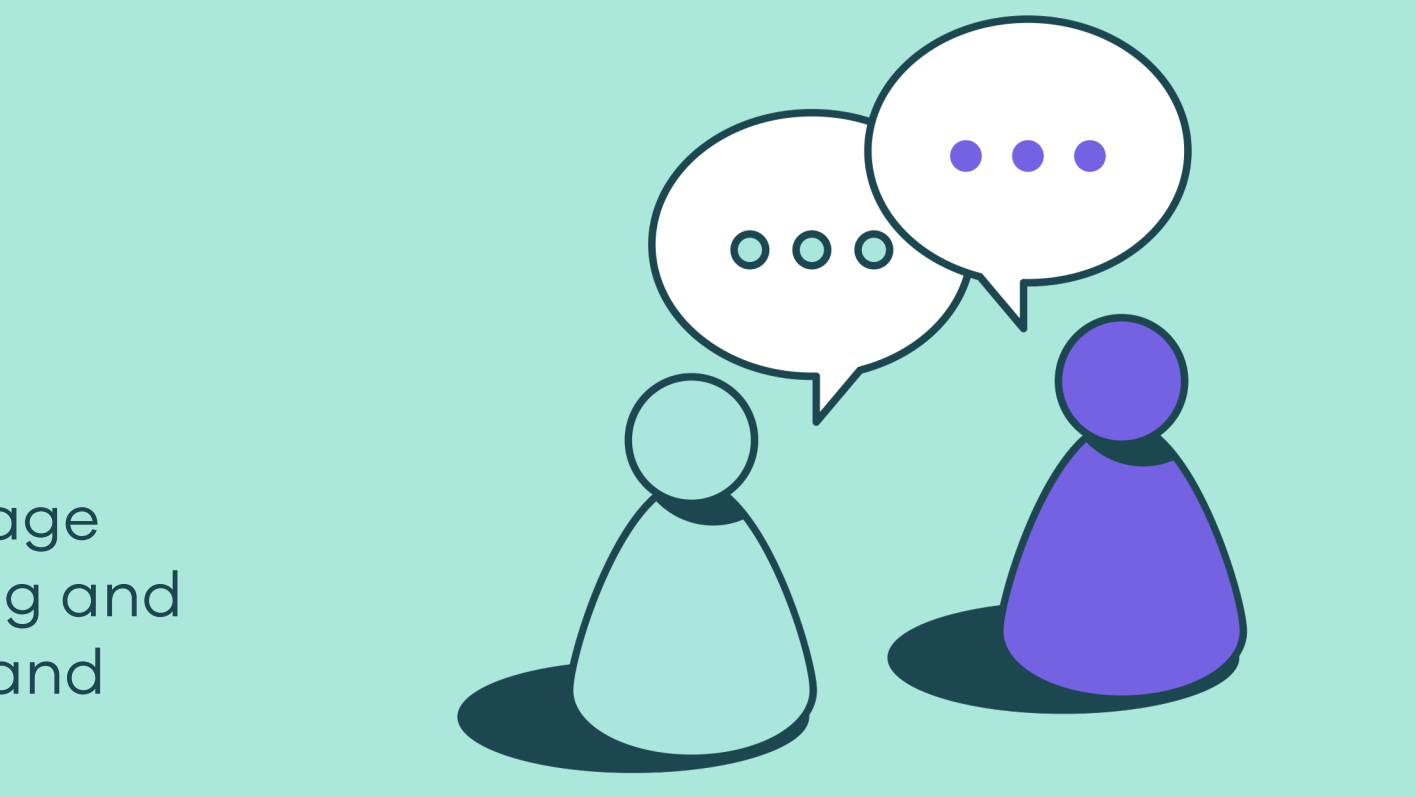
Take Moment To Own it this Cyber Smart Week:



Translated content

As part of 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 haumaruru 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](#).

Thank you

For helping to encourage everyone to take a moment
to own it to stay secure online.

If you have any questions about getting involved with Cyber Smart Week,
please reach out to us – we're happy to help: cybersmart@ncsc.govt.nz