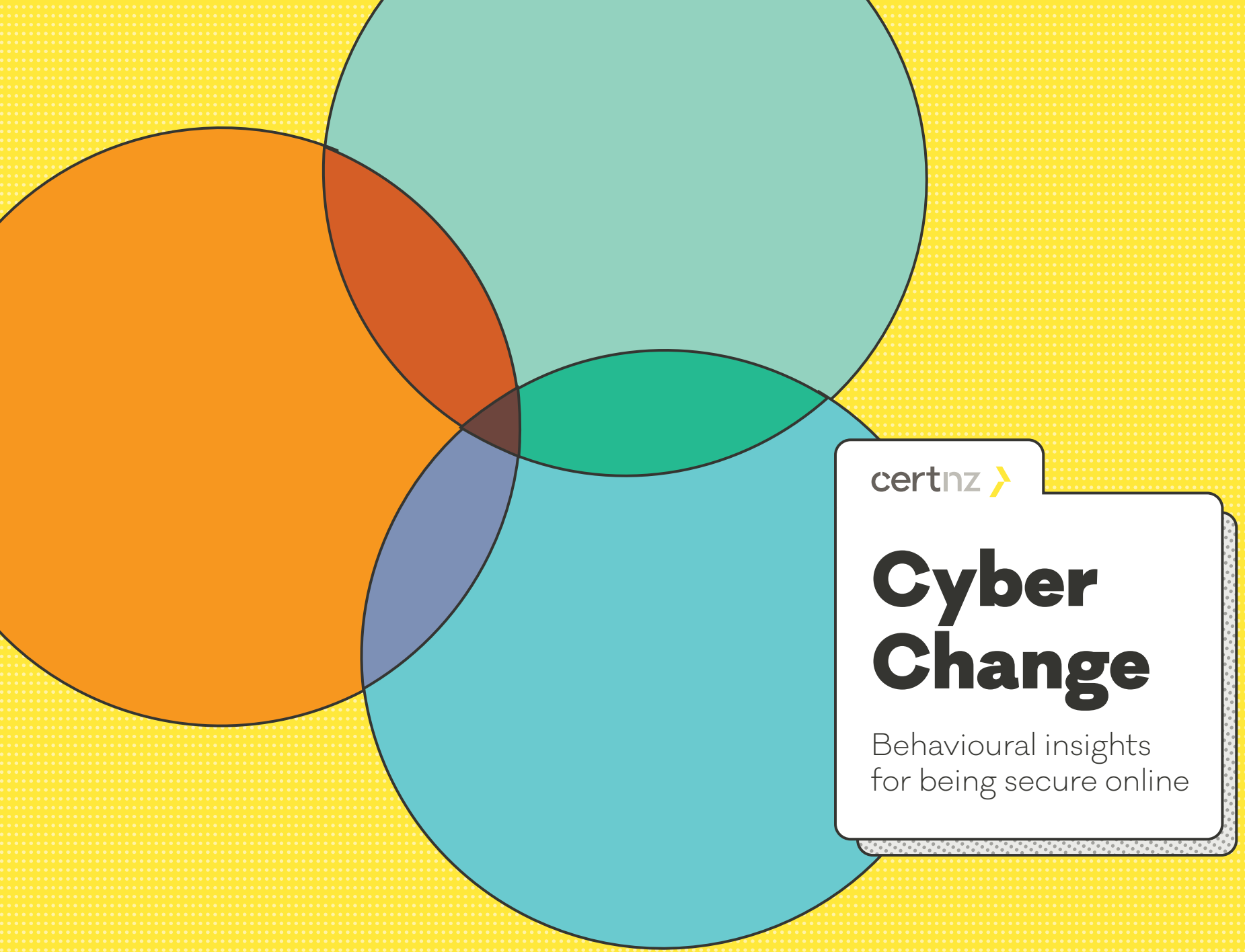


certnz

Cyber Change

Behavioural insights for being secure online

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

Introduction 4

COM-B behaviour change model 8

Cyber security nudges 18

- Capability 20
- Opportunity 34
- Motivation 48

Guide to nudging 62

End notes 66

Introduction

This guide was developed by CERT NZ and The Research Agency*.

We have created *Cyber Change* to offer insights and spark ideas among organisations and others working in security awareness to help nudge New Zealanders to be more secure online.

***You can read more about us on page 70, and more about the research methodology on page 68.**

The challenge

Many New Zealanders view cyber security as something for the tech-minded, but the reality is everyday people are at the centre of it. New Zealanders are increasingly experiencing cyber security incidents, and as a result are losing their money, information and privacy.

The good news is many cyber security incidents can be prevented, or have less impact, when protective measures are put in place. This includes seemingly simple actions like changing privacy settings in social media and using long, strong and unique passwords.

Although we say these actions are simple, people aren't always taking them despite their best intentions – and there isn't one single reason for this. A number of barriers prevent people from taking action to improve their online security. For example, some people don't believe cyber security threats are relevant to them; where as others aren't aware of how and why cyber security incidents happen. Some underestimate the possible impacts these incidents can have or aren't aware what steps they can take to protect against them.

Behavioural science can play a role in understanding and overcoming these barriers and unlocking opportunities to help people take action and better protect themselves online.

A behavioural science approach

What nudges are

Human behaviour is complex and people don't always act in a way that is straightforward. Our behaviour is affected by emotions, social factors, our environment and importantly, cognitive biases. Nudging draws on the understanding of cognitive biases and the wider field of behavioural science – a growing body of research based on psychology, neuroscience and economics.

Cognitive biases are our brain's mental short cuts. Biases guide our decision making and influence our behaviour without us even being consciously aware they are doing so. Biases can be helpful – sticking with the status quo and buying the same things we always buy helps us save time and know what to expect - but biases can also hinder us. In some instances, they can lead us to make rash decisions or prevent us from taking action when we most need to.

A nudge is an intervention that steers individuals towards a desired action. Nudging and behavioural science can help us harness the cognitive biases working in our favour and can help overcome the biases that hinder us.

Why we use nudges

Effectiveness

Small changes in context can have a dramatic impact on behaviour change. They can be a cost-effective way of enhancing campaigns, policies and service interventions to achieve better outcomes.

Grounded in human behaviour

Nudges and the field of behavioural science look beyond awareness raising and siloed thinking. They draw on a broad range of psychological, social and behavioural constraints; an understanding of human behaviour is at the core of this field.

From intention to action

Despite best intentions and preferences, people frequently don't act on them. Nudges help overcome the intention-action gap and drive behaviour change.

From micro to macro

Micro prompts and nudges can be guided by a broader behaviour change model to have an even greater and more systemic change. We can apply a range of nudges using the COM-B behaviour change model.

A model for behaviour change:

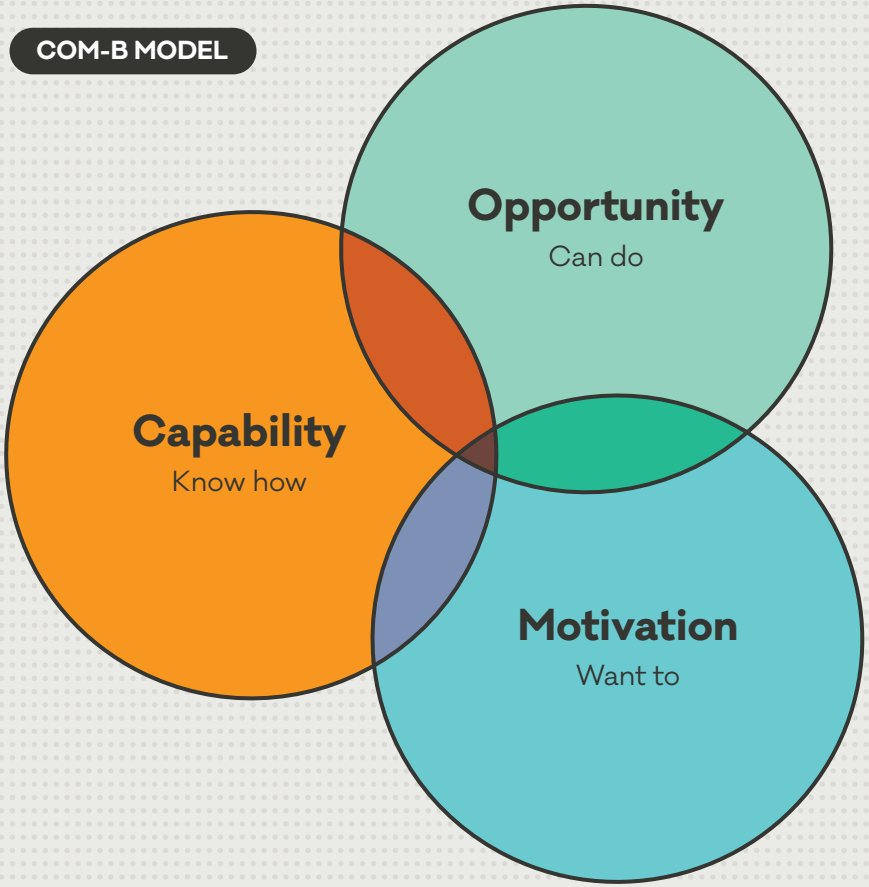
COM-B

Behaviour change is complex with no one solution. Raising awareness and building motivation, while important, are not always enough to encourage enduring behaviour change. Despite people's best intentions there are other factors that influence whether they will take action or not.

The COM-B behaviour change model recognises that behaviour is affected by a number of different factors and allows us to look at behaviour change at a more holistic level. If we are to influence behaviour (B), we need to consider capability (C), opportunity (O) and motivation (M).

The model was developed by Susan Michie, Professor at University College London, United Kingdom, where she is Director of the Centre for Behaviour Change. Professor Michie and her team led a systemic literature review of 19 different behaviour change models and synthesised the findings into the COM-B model.[1]

COM-B MODEL



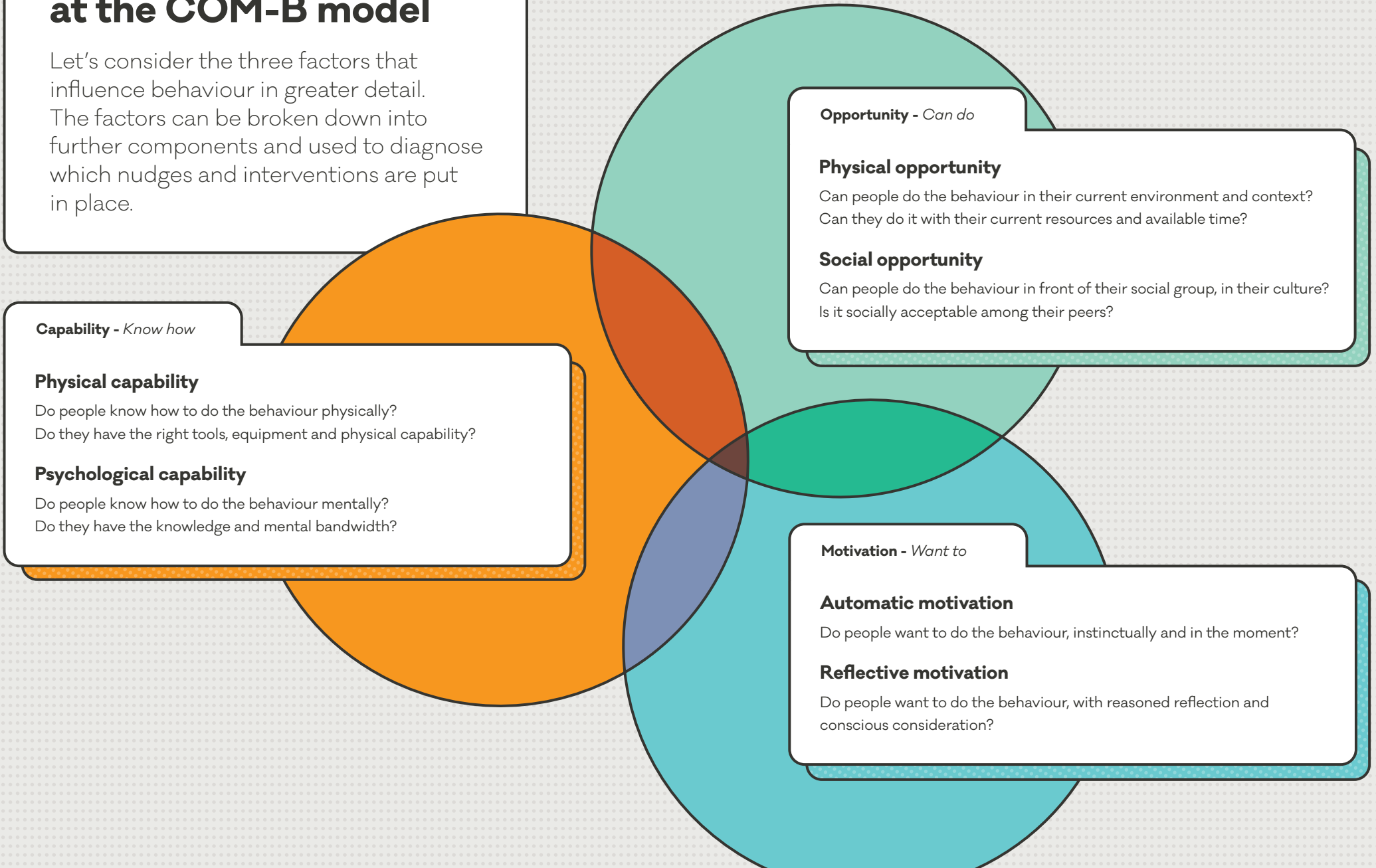
The COM-B model can be described as the 'know how, can do, want to' of behaviour change.

When developing nudges we need to consider whether we're addressing the following questions.

- Do people have the capability – the know how?
- Do people have the opportunity – the can do?
- Do people have the motivation – the want to?

Taking a closer look at the COM-B model

Let's consider the three factors that influence behaviour in greater detail. The factors can be broken down into further components and used to diagnose which nudges and interventions are put in place.



Capability - *Know how*

Physical capability

Do people know how to do the behaviour physically?
Do they have the right tools, equipment and physical capability?

Psychological capability

Do people know how to do the behaviour mentally?
Do they have the knowledge and mental bandwidth?

Opportunity - *Can do*

Physical opportunity

Can people do the behaviour in their current environment and context?
Can they do it with their current resources and available time?

Social opportunity

Can people do the behaviour in front of their social group, in their culture?
Is it socially acceptable among their peers?

Motivation - *Want to*

Automatic motivation

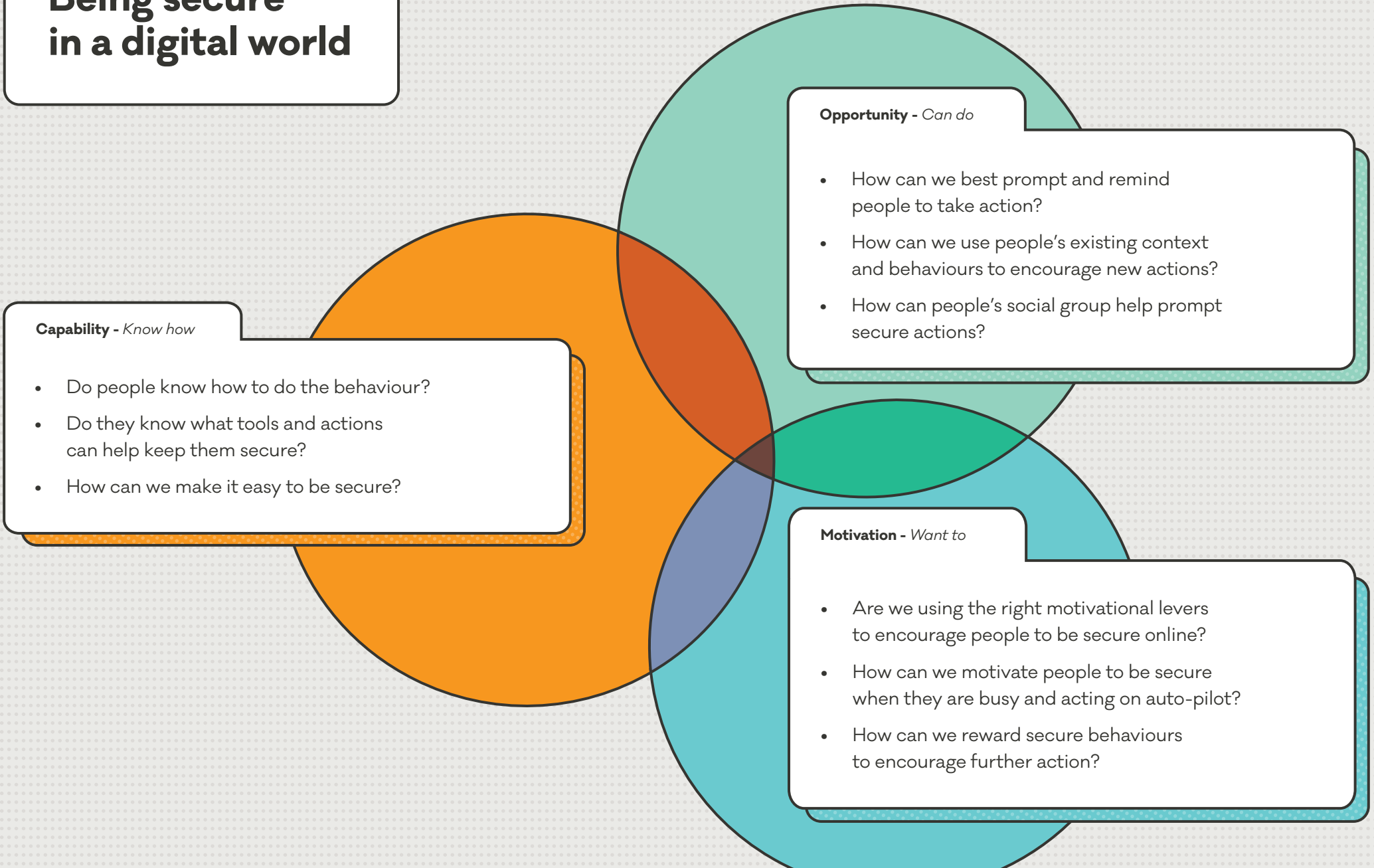
Do people want to do the behaviour, instinctually and in the moment?

Reflective motivation

Do people want to do the behaviour, with reasoned reflection and conscious consideration?

APPLYING COM-B

Being secure in a digital world



Common online security barriers to overcome

CAPABILITY barriers

Perceived effort

Despite the fact that some cyber security actions are simple and straightforward, there is a perception that being secure online requires effort and upkeep.

Complexity

While some are simple, other cyber security actions are more complex. Many people don't have the knowledge of how password managers or two-factor authentication (2FA) work, and find them too difficult to use.

Low confidence

Capability can refer to people's mental understanding and confidence. Saying 'no', hanging up or pausing to verify a phone scammer requires confidence and understanding that not everyone has.

OPPORTUNITY barriers

Intention-action gap

Despite people's best efforts and intentions, they will often forget or will delay their online security actions, like turning on 2FA or updating their software.

Untrusted sources

People are often getting advice from friends, family or informal sources. This advice, while well-intentioned, is not always sound.

Lack of salience

People lead busy lives and cyber security is not always a salient issue. This lack of awareness and appreciation for the importance of cyber security can be a barrier to action.

MOTIVATION barriers

Overly optimistic

Despite a prevalence of online threats, people are still overly optimistic. Many believe that an attack won't happen to them and if something were to happen, the consequences wouldn't be dire. As a result, the motivation to protect themselves online is low.

Overconfident

People are taking some actions to protect themselves online, for example, looking for secure payment settings when shopping online. However, they are overly confident that the small number of actions they are taking will fully protect them. As a result, the motivation to do more is low.

Low individual motivation

For some audiences, there is a sense that being proactive with cyber security is not up to them as an individual, rather it is the responsibility of their bank, workplace, government or other large players to act.

Defining the key behaviours

A key part of behaviour change and using the COM-B model is understanding what behaviours need to be influenced.

In the case of online security, there are many actions people can take to protect themselves, from creating long and strong passwords through to regularly updating security software across all devices.

On the following page are the key recommended online security behaviours this guide focuses on. Please note: this is not an exhaustive list of potential online security behaviours.

Online security behaviours

Authentication

- Using long and strong passwords
- Using different passwords for each online account
- Using two-factor authentication
- Using a password manager

Keeping systems up to date

- Updating software, browsers and apps to the latest version
- Installing and running cyber security software or apps on devices

Sharing information

- Not sharing personal information online with unknown people
- Setting social media accounts to private

Double checking trusted sites and payments

- Only making purchases from websites that use trusted and secure payment systems
- Verifying links in text messages and emails that are not from trusted and familiar sources before responding or clicking
- Reading customer reviews and feedback online to check if a website is legitimate

Reporting

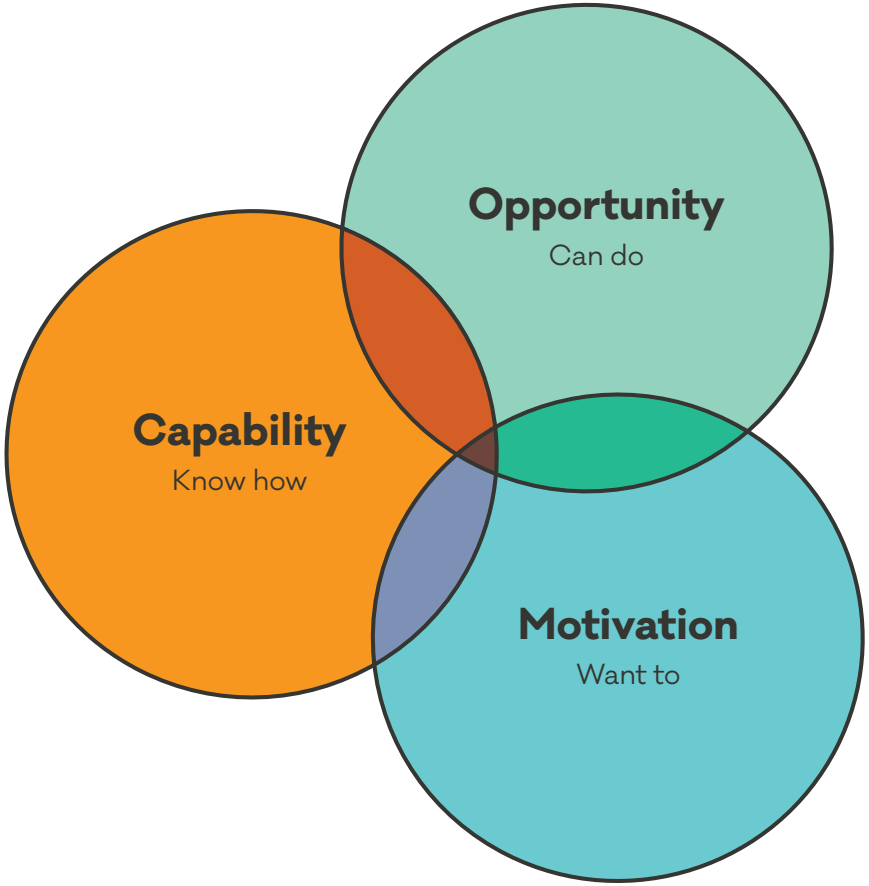
- Reporting an online threat, attack or crime

Other

- Staying up to date with online security advice from official sources
- Changing default password settings on devices like routers
- Using a VPN (virtual private network) when using public WiFi

Cyber Change

18 behavioural insights for being secure online using the COM-B behaviour change model



CAPABILITY

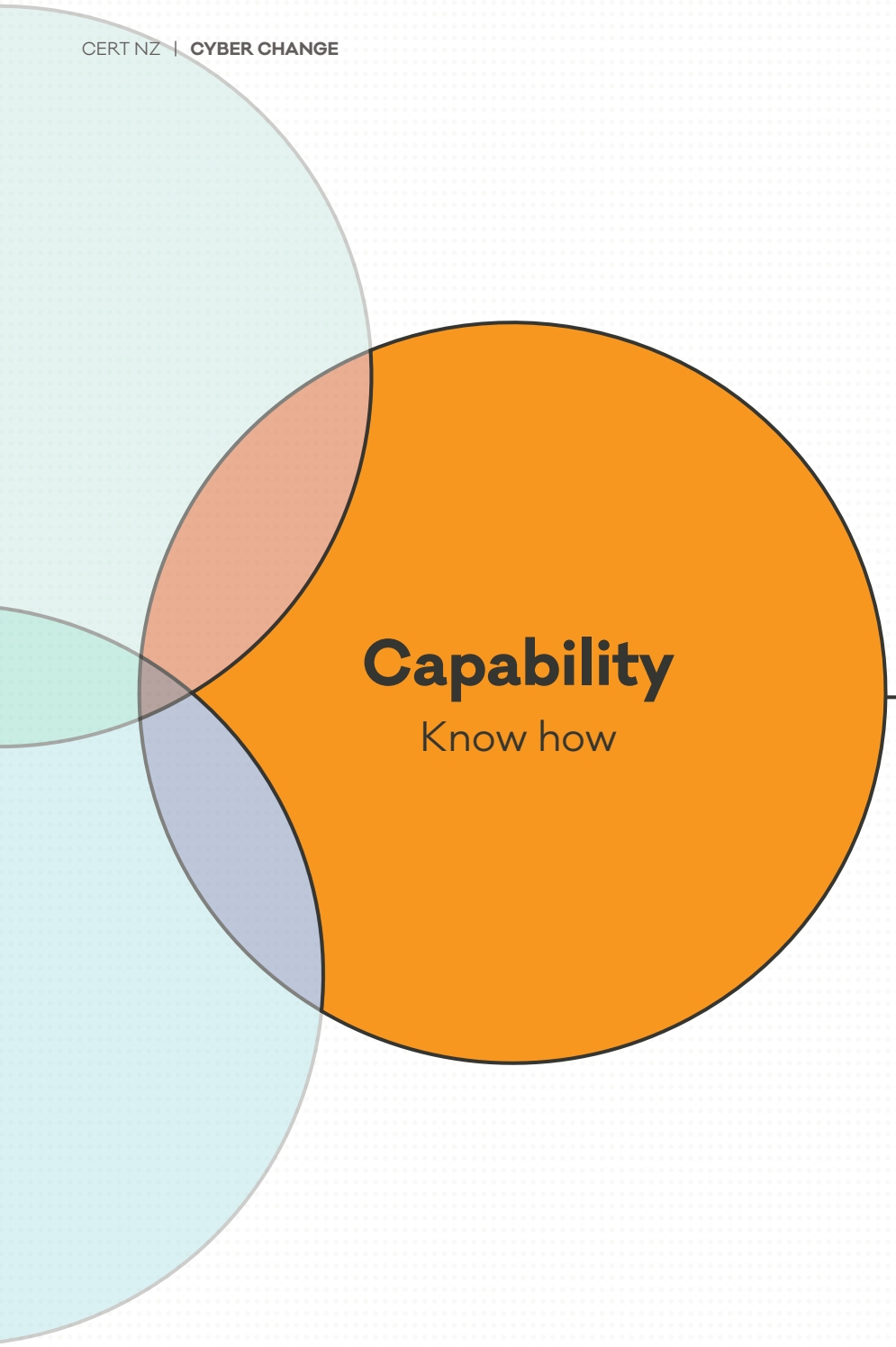
- Make it the default
- Overcome ambiguity
- Framing
- Make it socially acceptable to say 'no' to phone-scam callers
- Chunking information
- Make it easy to report

OPPORTUNITY

- Fresh starts
- Authority bias
- Social norms
- Availability heuristic
- Salience
- Habit stacking

MOTIVATION

- Make it human
- Make it tangible
- Make it collective
- Double-check mindset
- Use powerful analogies
- Provide feedback



- **Make it the default**
- **Overcome ambiguity**
- **Framing**
- **Make it socially acceptable to say ‘no’ to phone-scam callers**
- **Chunking information**
- **Make it easy to report**

CAPABILITY

Make it the default

Behavioural insight

A default is the pre-determined option. When choices and actions are difficult or easy to delay, defaults can guide the recommended behaviour.[2] For example, when the default for new employees was changed so they were automatically enrolled in a retirement saving scheme and having to opt out was an active step, participation increased by over 25%.[3]

Nudge

Many people know that they should be taking precautionary steps, like updating software and using 2FA, but don't often follow through with their intention.

Encourage key providers and partners to make sure their accounts and interfaces require a long and strong password with 2FA. In addition, make sure security updates for devices and apps happen automatically or are opt-out rather than opt-in.

Behaviour

Passwords, 2FA, updating software and devices

Audience considerations

Well suited for those who have low motivation to act

Responses to security updates being set to happen overnight as the default:

"I love this idea because it makes updating not a job and you don't have to make time for it."

"Absolutely yes!! I just forget and I would not go without my phone during waking hours to run an update."

"My settings are set so they automatically do it at like 2am when I'm asleep and I really like it because I don't have to manually update."

CAPABILITY

Overcome ambiguity

Behavioural insight

People tend to avoid uncertainty and ambiguity, preferring what is known and understood.[4] In the context of online security, key behaviours like using password managers and, for some audiences, using 2FA are not well known or understood, and people are hesitant to take up these steps.

Nudge

Overcome the uncertainty and ambiguity of using password managers and 2FA by showing people what to expect and how to use them. How-to videos, referrals from a friend and workplace demonstrations can help overcome the uncertainty of using something new.

Behaviour

Passwords, password managers, privacy settings, 2FA, updating software and devices

Audience considerations

Well suited for those who have low motivation to act

Responses to overcoming ambiguity

"I would be interested in videos that show me how to do it and explains what it is."

"I went and watched these videos, and a few others, and will now be setting up a password manager for myself!"

CAPABILITY

Framing

Behavioural insight

Our decisions and behaviours are influenced by the way information is framed. The same information can be perceived differently depending on what features are highlighted. A yoghurt that is framed as '90% fat-free' comes across very differently to one that is framed as '10% fat'. *How* something is said is as important as *what* is said.[5]

Nudge

We often talk about pass*words*, but reframing and referring to pass*phrases* can help people set up stronger protection that is also easier to remember. Likewise, reframing 'two-factor authentication' to 'two-step verification' can help people better understand the process. In addition, the term 'cyber' and 'cyber security' can have connotations of circuit boards, hooded hackers and the deep web, whereas 'online security' or 'being secure online' can be used as a more relatable, everyday term.

Behaviour	**Audience considerations**
Passwords, 2FA	Well suited for those who have low motivation to act

Responses to reframing 'password' to 'passphrase':

"I already use passphrases for my work and have implemented this in my personal life passwords too. I think a phrase makes it easier to remember and harder for bots to guess."

"I have never heard that term but I think it is a fantastic idea because of being so much easier to remember."

"Great idea...I have just started using this and will tell my friends."

CAPABILITY

Make it socially acceptable to say ‘no’ to phone-scam callers

Behavioural insight

Our social context influences our behaviour. We tend to follow social codes of conduct and stick to the norms, or what’s ‘socially acceptable’ among our peers, culture and wider society.[6] For example, it’s not considered socially acceptable to take your shoes off around strangers in a restaurant, but it is at home around friends and family.

Nudge

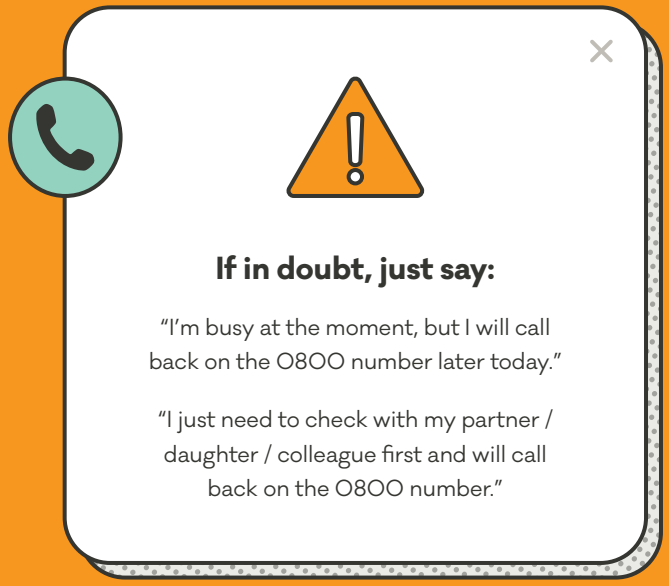
Some audiences find hanging up or saying ‘no’ to a scam caller difficult, awkward and, in some instances, impolite. Arming people with socially acceptable ways to say no to phone scams can help them end the call, be secure and avoid a possible incident.

Behaviour

Not sharing financial and personal information - for example, login details, credit card information.

Audience considerations

Well suited for those who have less confidence



Responses to socially acceptable ways to say ‘no’:

“These responses are helpful for people like me who are a bit passive in an unexpected situation.”

“I think these tactics are good. Scammers rely on us making fast decisions without consulting anyone else. They allow the person to be polite and firm.”

“Gives you some time and it’s a safe way not to accuse them of anything but to be able to double check.”

CAPABILITY

Chunking information

Behavioural insight

Chunking information reduces the perceived effort and can make a task easier. Sorting information into meaningful groups, categories or 'chunks' can not only reduce the perceived effort but also improve recall.[7] For example, when thinking about packing for a holiday, chunk the packing list into meaningful groups: clothes, toiletries, devices and travel documents.

Nudge

Rather than a long 'to-do list' of online security actions, chunk advice and the key recommended actions into meaningful groups. This shows people that being secure online can be simple with a handful of key actions.

Behaviour

All behaviours

Audience considerations

Well suited to a less confident and less capable audience

Responses to chunking information

"It's overwhelming. There's so much information and guidance out there."

"Make everything less complicated."

"Show that protecting yourself is simple."

"A simple three-or-four-step process."

CAPABILITY

Make it easy to report

Behavioural insight

Processes that are confusing or unknown and require high effort can prevent people from taking action. Simplifying a process and removing obstacles improves the cognitive ease and the likelihood of people completing the desired behaviour.[8]

Nudge

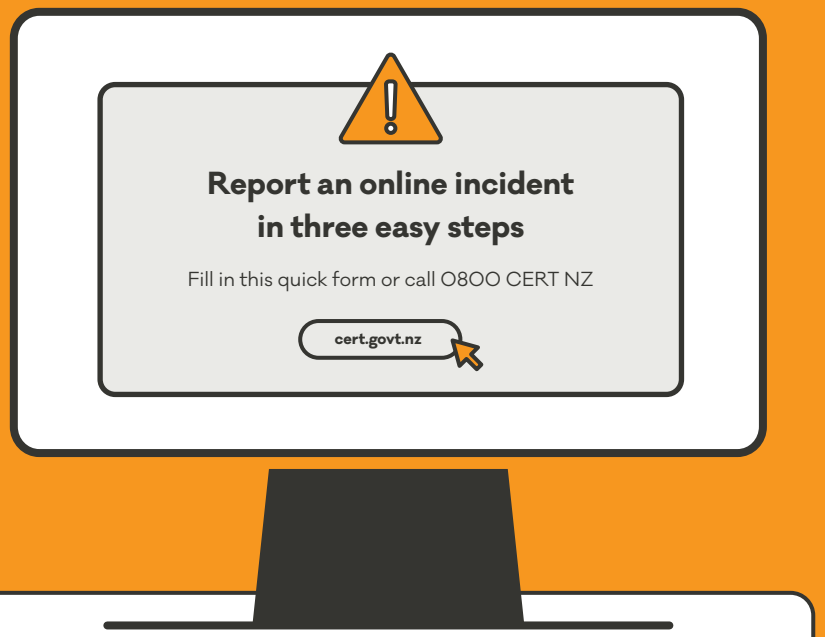
Make it easy to report an online security incident by keeping the process simple, short and seamless. Part of making it easy is also making it clear where to go to report an incident. In addition, dial up the motivation and give people more reason to report. For example, explaining up front that reporting helps protect other people from experiencing the same incident.

Behaviour

Reporting a cyber security incident

Audience considerations

Well suited for a broad audience



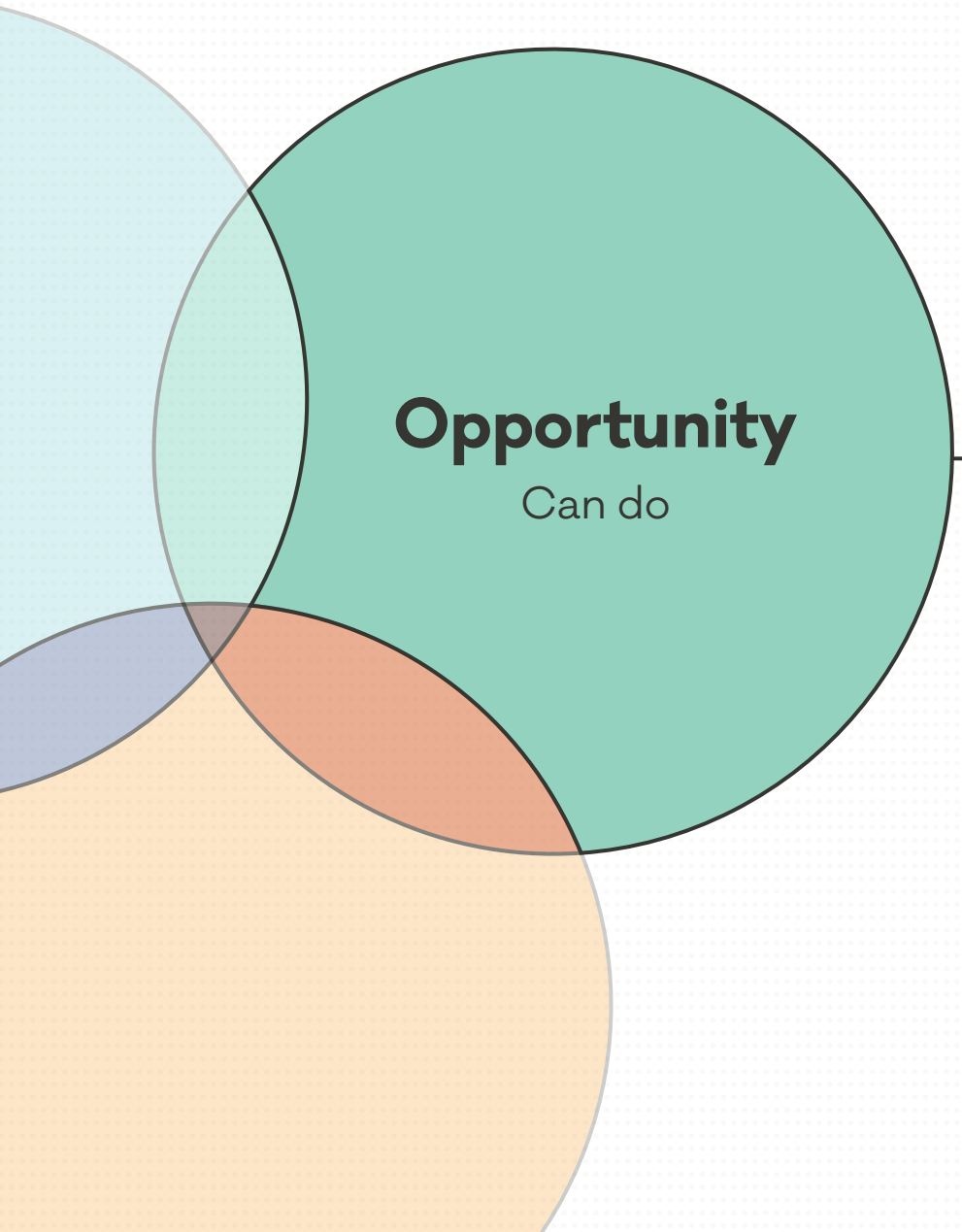
Responses to making it easier to report:

"Have a clear path on how to report."

"First off knowing where to actually report them."

"If there was one place you go to to lodge a complaint without all the drama."

"If it were an easy pop up on your phone like 'This message was from a unknown number, would you like to report it and block the number?'"



- **Fresh starts**
- **Authority bias**
- **Social norms**
- **Availability heuristic**
- **Salience**
- **Habit stacking**

OPPORTUNITY

Fresh starts

Behavioural insight

The fresh start effect refers to special occasions or 'temporal landmarks'. These are key moments where people are more likely to reflect and take action. For example, New Year's Eve is a well-known fresh start for resetting goals.[9]

Nudge

There are key moments when implementing online security behaviours are more relevant to people. These align to fresh starts, like setting up a new device or a first-time login. For example, work with technology providers to use key moments, like when someone purchases a new device to provide relevant online security steps. This could be an 'online security welcome pack'.

Behaviour

Passwords, password managers, updating software and devices, 2FA

Audience considerations

Well suited for a broad audience regardless of capability and confidence

Moments where people are more likely to implement online security measures:

Setting up a new device	63%
Setting up a financial service	48%
Signing up to a new website	44%

CERT NZ Cyber Security Research Apr 22; Q: We would like to understand the moment in which you typically implement cyber security measures. From the list below, please select which apply. Base: New Zealanders total sample n=1,217

OPPORTUNITY

Authority bias

Behavioural insight

It's not just the message that matters, but also who it's from. Authority bias is our tendency to give greater weight to information provided by authority figures. Authority can come in the form of experts, people or organisations with high social standing, and is indicated through symbols and signals of trust and authority, like trusted seals, ticks of approval or uniforms.[10]

Nudge

In the context of online security, key messengers and trusted sources of authority are financial institutions, internet and technology providers, workplaces and government agencies. However, people are not always using these messengers as sources of information. Make sure messaging and communication is coming from these trusted sources.

Behaviour

All behaviours

Audience considerations

Well suited for a broad audience

OPPORTUNITY

Social norms

Behavioural insight

Other people's actions can influence our own behaviour. We tend to conform to the behaviour of those around us, also known as social norming. We will often conform to groups we feel connected to, like our friends, family and colleagues.[11]

Nudge

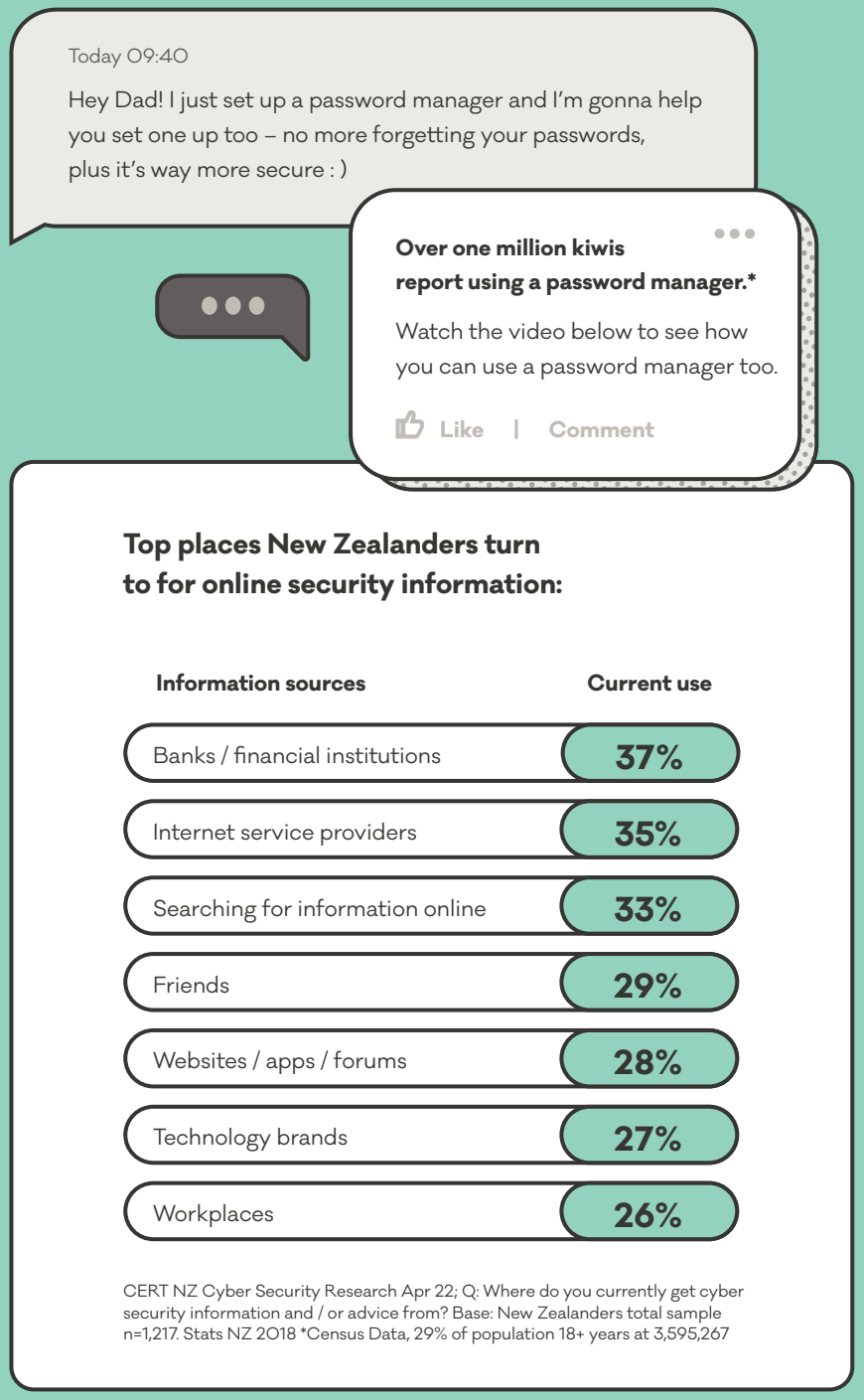
Pave the way for people to take action by showing that others are protecting themselves online. Use relevant 'people like me', like friends, family, colleagues, and trusted authority figures. For example, workplace IT departments, financial and internet service providers. To dial this up even further, provide friends, family and workplaces with trusted content and information they can share – help people to support those around them.

Behaviour

All behaviours

Audience considerations

Well suited for those who are more likely to help others. For example, those with higher capability and workplaces with staff working online.



OPPORTUNITY

Availability heuristic

Behavioural insight

The availability heuristic is our tendency to act off information that easily comes to mind. This is strongly linked to what media, advertising and news people are exposed to.[12] News stories can prompt the availability bias. For example, households are more likely to prepare for a natural disaster after seeing widespread coverage of an earthquake.

Nudge

Use the availability heuristic by following through with advice on how to be secure online following a significant online threat that is being covered by the media. People are more likely to acknowledge the risk of online threats and act after hearing about a cyber attack.

Behaviour

All behaviours

Audience considerations

Well suited to a broad audience. Well suited for workplaces to implement.

To: All staff

From: IT department

Subject: Now's the time to secure your online accounts

You may have seen the news about a large scale cyber attack impacting Organisation A.

Although our workplace is not directly at risk, it's a timely reminder to make sure you are:

- using long, strong and unique passwords across your online accounts (including your work email)
- turning on two-step verification where possible

For help in doing this, go to your Office Hub and see the how-to videos.

Thanks,
IT Department

Moments where people are more likely to implement online security

CERT NZ Cyber Security Research Apr 22; Q: We would like to understand the moment in which you typically implement cyber security measures. From the list below, please select which apply. Base: New Zealanders total sample n=1,217

OPPORTUNITY

Salience

Behavioural insight

The salience bias is our tendency to focus on information that either stands out, is novel or is more relevant to us.[13] Salience is often associated with strong visual cues, like the size/scale, colour, luminance and movement of key information.

Nudge

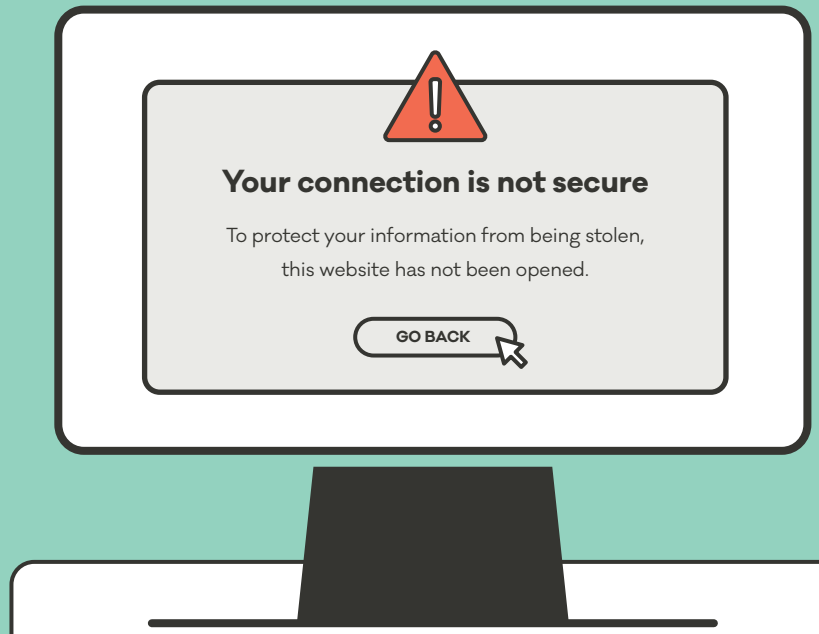
In the context of online security, pop ups, alerts, notifications, key use of colours (green for safe, red for unsafe) and symbols of trust (padlocks and shields) can all increase the salience of security features. Continue to increase the salience bias in relation to less secure sites, apps and forums to help alert people when they are at risk. Work with key providers and partners to make sure their sites and interfaces have implemented salient alerts for potential threats and risks.

Behaviour

Updating apps and software, passwords and verifying trusted sites and payments

Audience considerations

Well suited to a broad audience



"Users should expect the web is safe by default, and they'll be warned when there's an issue...

[Google will show] the red "not secure" warning when users enter data on HTTP pages"[14]

Emily Schechter, Product Manager, Chrome Security
2018

OPPORTUNITY

Habit stacking

Behavioural insight

Habits are automatic, repeated behaviours that often happen while we're on autopilot. Habit stacking is using an existing habit (for example cleaning your teeth) to prompt a new habit (flossing your teeth). As habits are regular and ongoing behaviours, habit stacking can be an effective way of regularly prompting a new behaviour.[15]

Nudge

In the context of online security, there are ongoing habits that can be used to prompt the desired online security behaviours. These can be general habits, like spring cleaning, check ups or WOFs, but they can also be more relevant habits.
For example, financial habits, like tax returns, checking bank accounts, or updating bank cards. They also could be online habits, like shutting down a device for the night.

Behaviour	**Audience considerations**
All behaviours	Well suited for a broad audience

Checking your savings account?

Be sure to check your account security too, here's how:

- use a long, strong, unique password
- turn on 2FA. go to your account settings for more information on how to do this

Go to your account settings for more information on how to do this.

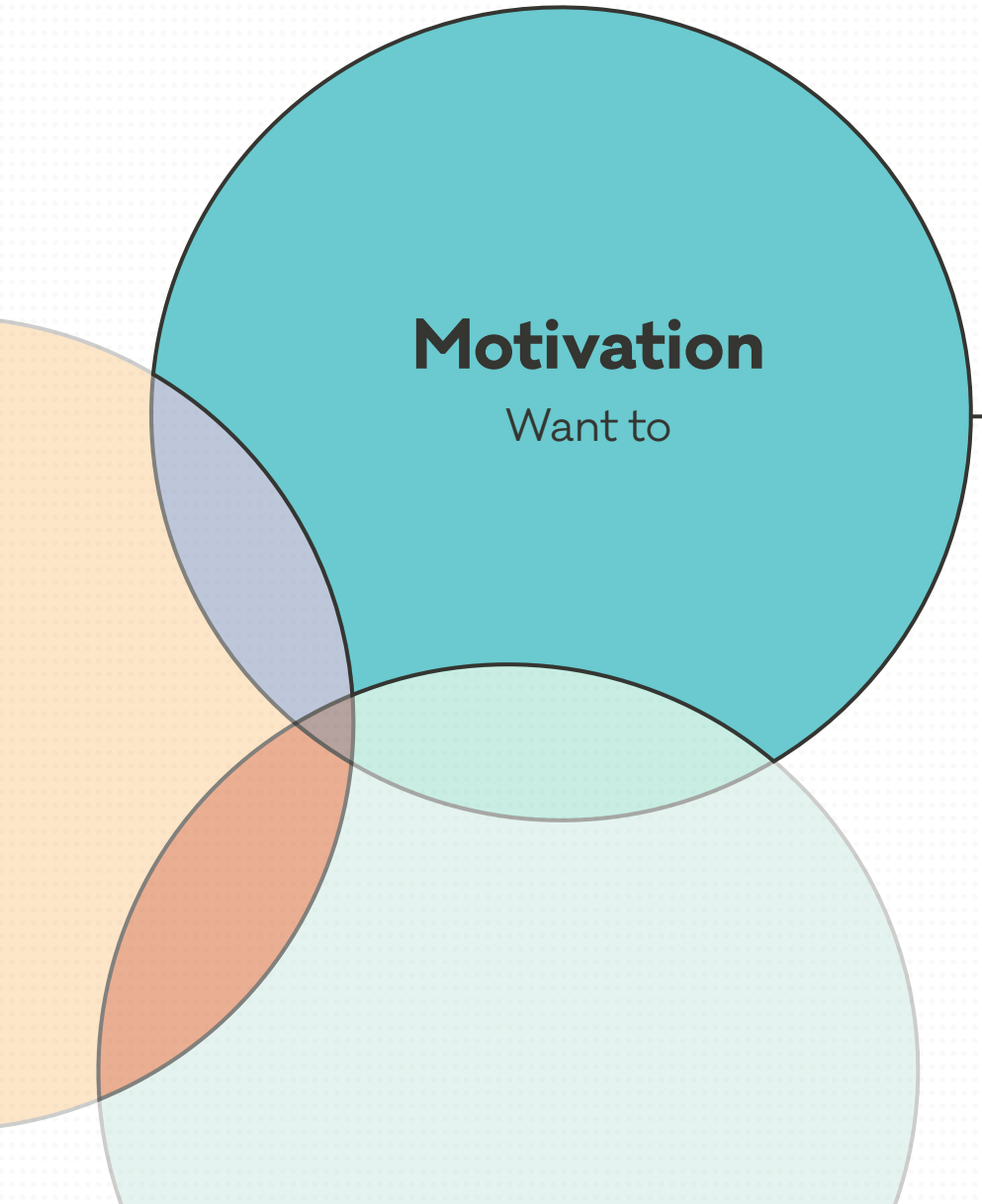
Responses to habit stacking;

"Tying it to a season means it can be done regularly. Like the smoke alarm check."

"For me, personally I find cyber security is front of mind when I'm doing tax returns online and needing to upload stuff and attach documents."

"Front of mind/important is when there is financial involvement."

"I think it's good to have a reminder when you are finishing off work or shutting down for the day."



- **Make it human**
- **Make it tangible**
- **Make it collective**
- **Double-check mindset**
- **Use powerful analogies**
- **Provide feedback**

MOTIVATION

Make it human

Behavioural insight

People's behaviour and decision making is affected by priming. Priming is the exposure to certain stimuli, like imagery or certain types of words and language. For example, priming people through exposure to words like athletic, fit, lean and the concept of being active makes them more likely to take the stairs than the lift.[16]

Nudge

Cyber security is currently presented in the media as dark, shadowy and complex; and something for experts, IT specialists and large organisations to deal with. Consider priming for a more human, everyday 'people like me' and empowering tone. Use imagery, language and tone to subconsciously motivate people into action.

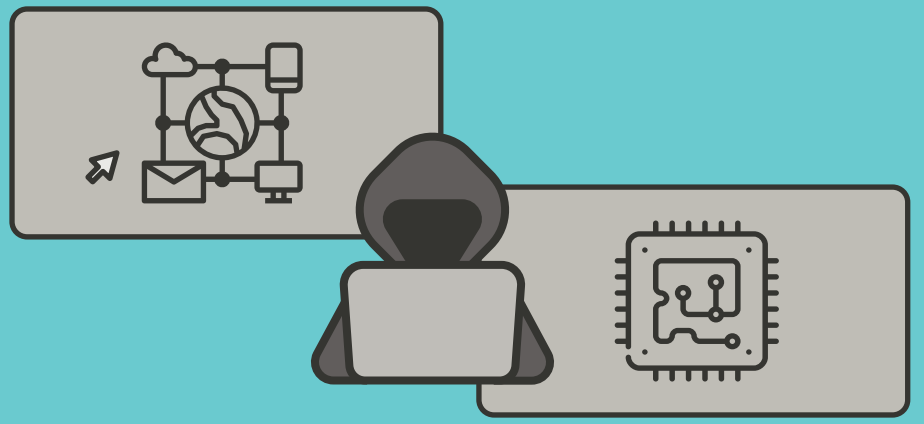
Behaviour

All behaviours

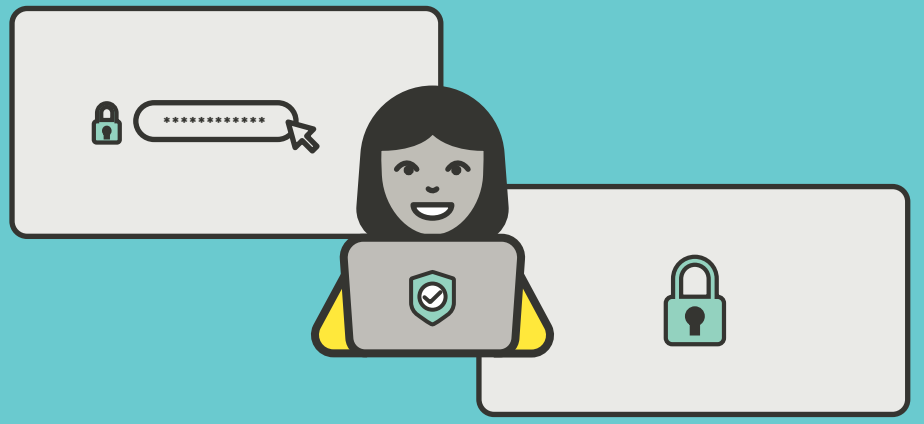
Audience considerations

Well suited for those who have low cyber and tech capability and confidence

FROM → Dark, shadowy, complex



TO → Human, easy, empowering



MOTIVATION

Make it tangible

Behavioural insight

Loss aversion is a cognitive bias that refers to people's tendency to prefer avoiding a loss or risk to acquiring a relevant gain – losses seem larger than gains.[17] For example, avoiding a $5 surcharge is more motivating than gaining a $5 discount. Loss aversion taps into people's risk aversion and threat avoidance.

Nudge

People can have a low perception of the risks that online security threats can cause and may tend to be overly optimistic (taking the 'she'll be right' attitude) and overconfident in their actions when it comes to online security. Therefore, we need to make the consequences of online threats more tangible to people and show why it's important to take action.

Despite increasing attacks, threats can feel abstract and distant – there is a sense of 'it won't happen to me'. Additionally, many people don't fully grasp the consequences of digital identity loss. Without overt fear mongering, the tangible consequences of online threats should be dialled up, with a particular focus on the consequences of digital identity theft.

Behaviour

All behaviours

Audience considerations

Well suited to a broad audience

FROM → Focusing on just 'what to do'

Be secure online

Avoid sharing information
with people you don't know

TO → What to do and show why it's important

Your personal information (name, address, DOB) is valuable information to cyber attackers.

They can use this to try and access your online accounts and impersonate you online.

Protect your identity online
Avoid sharing information
with people you don't know

CERT NZ

MOTIVATION

Make it collective

Behavioural insight

Social norms are the rules and expectations that guide the behaviour of a social group or a particular society. Social norms can often encourage pro-social behaviour – we tend to act with reciprocity towards those who are in our social group.[18] An example of using pro-social motivations is framing the COVID-19 vaccination to protect vulnerable people in the community.

Nudge

Show that being secure online is something we can do with others, and for others. Make online security collective 'with others' by showing that we're all in this together and many people and organisations are working to combat online threats. This helps build a sense of momentum and herd behaviour. Make it collective 'for others' by showing that taking action, reporting online attacks and supporting the less cyber savvy can protect others.

Behaviour	**Audience considerations**
All behaviours	Well suited to a broad audience

FROM → Focusing on just 'what to do'

Protect yourself online

Make sure you have long and strong passwords

Turn on two-step verification

TO → What to do and collective messaging

We're protecting our customers from cyber crime - here's how you can help too!

Make sure you protect your accounts with long, strong passwords

If your social media accounts get hacked, your mates could be at risk too

Protect your social accounts with two-step verification

MOTIVATION

Double-check mindset

Behavioural insight

The dual-system model contrasts System 1 thinking – fast, automatic and sub-conscious (for example, brushing your teeth, tying a shoelace) - with System 2 thinking – slower, conscious, and requiring more effort to solve more complicated challenges (for example, choosing between insurance plans).[19] While System 1 thinking is fast and reflexive, it can be advantageous to prompt people into a more conscious thought process for more reasoned thinking and decision making.

Nudge

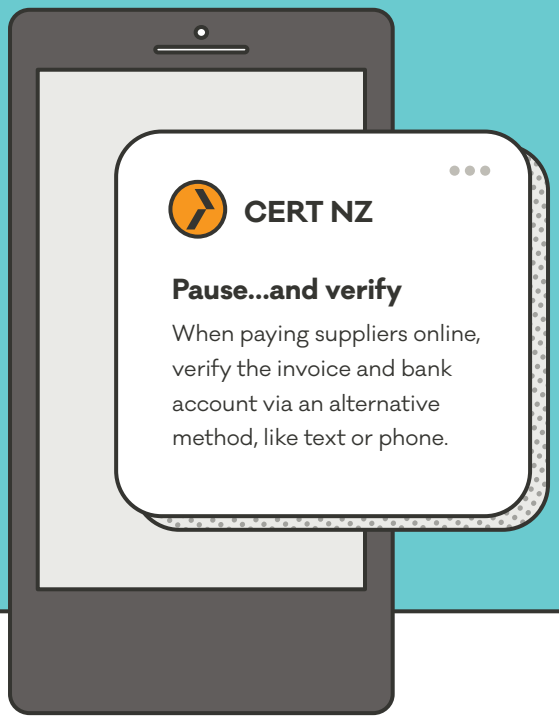
People are usually more vulnerable to scams and phishing when they're busy and on 'autopilot' mode (during System 1 thinking). Even the most security conscious and capable people can be impacted when they're not paying attention. Encouraging a double-check mindset, and getting people to pause and verify, can help people switch from System 1 autopilot to a more alert and discerning System 2 approach.

Behaviour

Verify communications are legitimate before taking action

Audience considerations

Well suited for a broad audience and especially those who may be busy, distracted and/or complacent.



Responses to a double-check mindset:

"If you weren't expecting it, suss it out. You look before you jump, so check before you click."

"We get so busy we can just click something open and before we know it we are down a rabbit warren... it's definitely helpful to stop and think before you open things."

"If people are asked to stop and look, and possibly given the example of the consequences if they hadn't taken a pause to check the scenario, then it might drive home the importance of checking."

MOTIVATION

Use powerful analogies

Behavioural insight

Presenting information through analogies and metaphors can help shape how we think about a topic, and in turn, how we behave. For example, when the brain is described as a 'muscle' that can 'grow' with practice, students are more likely to understand that intelligence is not fixed, making them more committed to their learning goals.[20]

Nudge

Use framing and powerful analogies to bring new meaning to key actions that can help people be secure online. We know people don't always grasp the potential risks or threats they're exposed to, but using analogies can help people understand the risks involved, and the required action. Use relevant risk-avoidance analogies, like physical safety and security, and preventative analogies like WOFs or spring cleaning.

Behaviour	**Audience considerations**
All behaviours	Well suited to a broad audience

FROM → Focusing on just 'what to do'

Be secure online

Don't share information online with people you don't know

TO → What to do and relevant analogy

MOTIVATION

Provide feedback

Behavioural insight

Providing individuals with information about the consequences of their past behaviour through feedback is an effective way to enhance learning and prompt greater motivation.[21] Whether it's showing students questions they answered incorrectly in a practice test to prompt more study, or getting a health result to encourage healthier choices, feedback can be an effective mechanism for encouraging behaviour change.

Nudge

Provide feedback to positively reinforce good behaviours. For example, provide positive feedback for enabling 2FA and when devices have been updated. As part of the positive feedback, reiterate why and how this behaviour has kept the person and others secure.

Build on this positive feedback nudge by including what next step can be taken to be even more secure online.

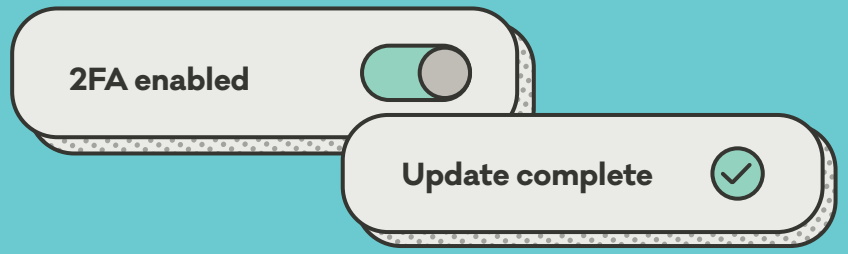
Behaviour

Passwords, updating devices and software, password managers, reporting, 2FA and privacy settings.

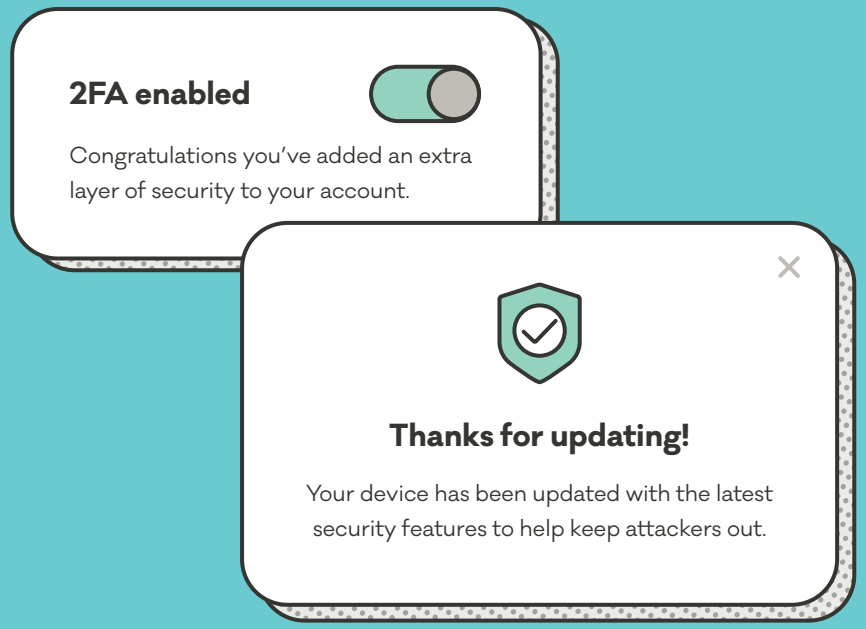
Audience considerations

Well suited for a broad audience and those who may be complacent

FROM → No feedback



TO → Providing positive feedback



Guide to nudging

A step-by-step guide for applying behavioural insights to being secure online.

Define — **Explore** — **Design** — **Test** — **Refine**

Define **Define the behaviour change objective**

What is the behaviour we're trying to encourage?

The audience: _____ (who/population)

The behaviour: _____ (what)

The conditions: _____ (when/where/how)

As measured by: _____ (indicators and to what extent)

Explore **Explore the context**
Using the COM-B model, explore the barriers and drivers of the desired behaviour.

CAPABILITY

- Do people know how to do the behaviour?
- Do they know what tools and actions can keep them secure?
- How can we make it easy to be secure?

OPPORTUNITY

- How can we best prompt and remind people to take action?
- How can we use people's existing context and behaviours to encourage new actions?
- How can people's social groups help prompt secure actions?

MOTIVATION

- Are we using the right motivational levers to encourage people to be secure online?
- How can we motivate people to be secure when they are busy, not interested and acting on auto-pilot?
- How can we reward secure behaviours to encourage further action?

Guide to nudging continued...

Design

Design the nudge.
Consider what nudge/s will be most effective for the desired behaviour and what can be feasibly implemented.

CAPABILITY

- Make it the default
- Overcome ambiguity
- Framing
- Make it socially acceptable to say 'no' to phone-scam callers
- Chunking information
- Make it easy to report

OPPORTUNITY

- Fresh starts
- Authority bias
- Social norms
- Availability heuristic
- Salience
- Habit stacking

MOTIVATION

- Make it human
- Make it tangible
- Make it collective
- Double-check mindset
- Use powerful analogies
- Provide feedback

Test

Test for effectiveness
Set a success measure and test the nudge for its effectiveness

Set a success measure

First determine what success looks like. To what extent are we trying to shift the behaviour? By how much? Which audience in particular?

Measure the outcomes

Determine how to best measure the success of the nudge. Capturing real behaviour is best practice, but reported data can still be valuable.

Trial first

Before it is rolled out at scale, run a test pilot to work out any issues in advance and to get preliminary results to work with.

Consider the wider context

Look out for knock on effects and wider influences at play. Consider timing of the test period and what events and activities are on at the same time. Consider and capture unintended consequences or flow-on effects as a result of the nudge.

Refine

Refine and scale
Gather lessons learned then look to scale up and build upon the nudge.

Refine

Analyse the results to determine the effectiveness of the nudge. Take the learnings to reassess and refine.

Scale up the nudge

Consider rolling out the nudge wider, in a different context and/or to a different audience. Consider what additional resources you will need to implement the intervention at a bigger scale.

Combine nudges for impact

The COM-B model is effective because it takes into account the different aspects of behaviour. Build upon one nudge by combining it with another nudge or a range of different nudges across the capability, opportunity and motivational spectrum.

End notes

1. Michie, S., van Stralen, M.M. & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. Implementation Science 6(1), 1-12. https://doi.org/10.1186/1748-5908-6-42
2. Thaler, R. H., & Sunstein, C. (2008). Nudge: Improving decisions about health, wealth, and happiness. New Haven, CT: Yale University Press.
3. Beshears, J., Choi, J., Laibson, D., Madrian, B., Kay, S.J. & Sinha, T. (2008). The importance of default options for retirement saving outcomes: evidence from the United States. Lessons from Pension Reform in the Americas, 59–87. https://doi.org/1093/acprof:oso/9780199226801.003.0004
4. Ellsberg, D. (1961). Risk, ambiguity, and the savage axioms. The Quarterly Journal of Economics, 75(4), 643-669. https://doi.org/10.2307/1884324
5. Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: A typology and critical analysis of framing effects. Organizational Behavior and Human Decision Processes, 76(2),149-188. https://doi.org/10.1006/obhd.1998.2804
6. Yamin, P., Fei, M., Lahlou, S., & Levy, S. (2019). Using social norms to change behavior and increase sustainability in the real world: A systematic review of the literature. Sustainability, 11(20). 5847. https://doi.org/10.3390/su11205847
7. Mathy, F., & Feldman, J. (2012). What's magic about magic numbers? Chunking and data compression in short-term memory. Cognition, 122(3), 346-362. https://doi.org/10.1016/j.cognition.2011.11.003
8. The Behavioural Insights Team. (2014). EAST: Four Simple Ways to Apply Behavioural Insights. https://www.bi.team/publications/east- four-simple-ways-to-apply-behavioural-insights/
9. Dai, H., Milkman, K. and Riis, J. (2014). The Fresh Start Effect: Temporal Landmarks Motivate Aspirational Behavior. Management Science, 1-20. http://dx.doi.org/10.1287/mnsc.2014.1901
10. Greer, J. (2003). Evaluating the Credibility of Online Information: A Test of Source and Advertising Influence, Mass Communication and Society, 6(1), 11-28, https://doi.org/10.1207/S15327825MCS0601_3. Knight Lapinski, M. & Rimal, R. N. (2005). An Explication of Social Norms, Communication Theory, 15(2), 127-147. https://doi.org/10.1111/j.1468-2885.2005.tb00329.x
11. Knight Lapinski, M. & Rimal, R. N. (2005). An Explication of Social Norms, Communication Theory, 15(2), 127-147. https://doi.org/10.1111/j.1468-2885.2005.tb00329.x
12. Pachur, T., Hertwig, R., & Steinmann, F. (2012). How do people judge risks: availability heuristic, affect heuristic, or both?. Journal of Experimental Psychology: Applied, 18(3), 314.
13. Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). MINDSPACE: Influencing Behaviour through Public Policy. Retrieved from: http://www.instituteforgovernment.org.uk/publications/mindspace
14. Schechter, E. (2018). Evolving Chrome's security indicators. Chromium Blog. Retrieved from: https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html
15. Fogg, B. J. (2020). Tiny Habits: The small changes that change everything. Boston, MA: Houghton Mifflin Harcourt.
16. Wryobeck, J., & Chen, Y. (2003). Using priming techniques to facilitate health behaviours. Clinical Psychologist, 7(2), 105-108. https://doi.org/10.1080/13284200410001707553
17. Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference-dependent model. The Quarterly Journal of Economics, 106(4), 1039-1061. https://doi.org/10.2307/2937956
18. Siu, A. M., Shek, D. T., & Law, B. (2012). Prosocial norms as a positive youth development construct: A conceptual review. The Scientific World Journal, 2012, 1-7. https://doi.org/10.1100/2012/832026
19. Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. American Economic Review, 93(5), 1449-1475. https://doi.org/10.1257/000282803322655392
20. Thibodeau PH, Hendricks R. K., Boroditsky L. (2017). How Linguistic Metaphor Scaffolds Reasoning. Trends in Cognitive Science 12(11), 852-863. https://doi.org/10.1016/j.tics.2017.07.001
21. Erev, I., & Roth, A. E. (2014). Maximization, learning, and economic behavior. Proceedings of the National Academy of Sciences, 111(supplement_3), 10818-10825. https://doi.org/10.1073/pnas.1402846111

Research methodology

A multi-stage, mixed methodology approach

Stage 1: Media discourse and analysis

TRA conducted desk research (over 30+ websites) across a vast number of sources where New Zealanders might encounter online security topics. This included the following sources:

- New Zealand media sites
- International news and magazine sites
- Social media sites
- Government websites
- New Zealand and overseas e-commerce websites
- Internal research documents and existing literature on cyber security awareness

Social media, scraping, was used by plugging in key words associated with online security, allowing TRA to generate a large number of individual articles and blogs (150+) that captured different conversations New Zealanders would be exposed to about online security. Media analysis was completed in February and March 2022. In addition, three cyber security experts were interviewed.

Stage 2: Quantitative

The survey interviewed a nationally representative sample of New Zealanders aged 18 years and over.

- Total sample n=1,217
- Margin of error at the 95% confidence interval was ±2.8%
- Fieldwork ran from 8 to 17 March 2022
- The data was post-weighted to be representative of the New Zealand population in terms of age, gender, region and ethnicity.

An additional survey was used to analyse small to medium-sized businesses ranging from 0 —100 FTE.

In addition, three interviews heads of security from with large organisations were interviewed.

Stage 3: Qualitative and behavioural analysis

A two-phase approach was taken to gain a deeper overall insight and nuance into our segments.

Focus group discussions

- 5 focus groups
- 5 per group, total of 25 participants
- 1.5 hours each session

Four-day monitored online tasks to understand behaviour

- Capturing participants' behaviours and perceptions of online security.
- Capturing behavioural responses to nudges and interventions.
- Literature review and behavioural analysis of the nudges and interventions.

Within the bounds of segment qualifying criteria, including a mix of location, age, gender and ethnicity across the sample.

About us

CERT NZ is New Zealand's Computer Emergency Response Team. We work to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. We provide trusted, authoritative information and advice, while also collating a profile of the threat landscape in New Zealand.

For more information see **cert.govt.nz**

TRA (The Research Agency) is an insights agency. We use our understanding of human behaviour to identify opportunities for organisations to grow.

While we make extensive use of research, data analytics, strategy and planning tools, the distinguishing feature of our work is our knowledge of human behaviour.

For more information see **theresearchagency.com**

Acknowledgements

This research was commissioned by CERT NZ and Department of the Prime Minister and Cabinet, Te Tari o te Pirimia me te Rūnanga Kāwanatanga (DPMC).

The authors were Lindsey Horne and Olivia Lacey.

We thank the research participants who took part in qualitative and quantitative research and the TRA research team who conducted the research.

We thank all those who reviewed this work, including DPMC, the wider CERT NZ team and Dr Marcos Pelenur.

Reproduction

Notes