Australian Government
Department of the Prime Minister and Cabinet

BETA

password123

Applying behavioural insights to cyber security advice

January 2021

Other uses

Enquiries regarding this license and any other use of this document are welcome at:

Managing Director
Behavioural Economics Team of the Australian Government
Department of the Prime Minister and Cabinet
1 National Circuit
Barton ACT 2600
Email: beta@pmc.gov.au

The views expressed in this paper are those of the authors and do not necessarily reflect those of the Department of the Prime Minister and Cabinet or the Australian Government.

Research team

Current and former staff who contributed to the report were: Ashley Breckenridge, Andrew Bromwich, Laura Bennetts Kneebone, Scott Copley, Shea Houlihan, Linda Ma and Andrea Willis.

Acknowledgments

Thank you to the Australian Cyber Security Centre for their support and valuable contribution in making this project happen. In particular, special thanks to Georgia Conduit, Emily Walker, Nicola Friedlieb, and Kelly Charls for their work on this project.

These trials were pre-registered on the BETA website and the American Economic Association registry:

AEARCTR-0005501 *Using Emails Effectively for Sharing Cyber Security Advice*

AEARCTR-0004957 *Engaging Small Business in Cyber Safe Practice*

AEARCTR-0005519 *Using Websites Effectively for Sharing Cyber Security Advice*

Who?

Who are we?

We are the Behavioural Economics Team of the Australian Government, or BETA. We are the Australian Government's first central unit applying behavioural economics to improve public policy, programs and processes.

We use behavioural economics, science and psychology to improve policy outcomes. Our mission is to advance the wellbeing of Australians through the application and rigorous evaluation of behavioural insights to public policy and administration.

What is behavioural economics?

Economics has traditionally assumed people always make decisions in their best interests. Behavioural economics challenges this view by providing a more realistic model of human behaviour. It recognises we are systematically biased (for example, we tend to satisfy our present self rather than planning for the future) and can make decisions that conflict with our own interests.

What are behavioural insights and how are they useful for policy design?

Behavioural insights apply behavioural economics concepts to the real world by drawing on empirically-tested results. These new tools can inform the design of government interventions to improve the welfare of citizens.

Rather than expect citizens to be optimal decision makers, drawing on behavioural insights ensures policy makers will design policies that go with the grain of human behaviour. For example, citizens may struggle to make choices in their own best interests, such as saving more money. Policy makers can apply behavioural insights that preserve freedom, but encourage a different choice – by helping citizens to set a plan to save regularly.

Contents

About this report

This report forms part of a series of reports on applying behavioural insights to improve cyber security advice for individuals and small businesses in Australia. The research and findings outlined in this series are the result of a number of projects BETA completed in partnership with the Australian Cyber Security Centre (ACSC) throughout 2019 and 2020. Relevant findings from across these different projects are presented according to theme:

- On the alert: Using behavioural insights to boost the impact of cyber security alerts;
- After the crime: Experiences of cyber security incidents
- **password123: Applying behavioural insights to cyber security advice [this report]**

Each report, along with the Technical Appendix for all three reports, are available on the BETA website: https://www.behaviouraleconomics.pmc.gov.au/projects

Executive summary

The risks of poor cyber security intensify as more aspects of people's lives and businesses become digitised and connected online. The methods cybercriminals use are more sophisticated than ever, meaning regular (non-expert) individuals and small businesses must also improve their ability to detect scams and protect their personal and business accounts and devices.

To help improve the impact of cyber security advice for individuals and small businesses, BETA partnered with the Australian Cyber Security Centre (ACSC) to design and test different formats of advice. We conducted focus groups and two survey experiments (surveys with embedded randomised controlled trials) to understand whether behavioural insights concepts are effective in shifting people's intentions to enact safer cyber security practices. We surveyed small and medium business (SMB) owners and operators and tested the effect of different formats of advice.

We developed plain text advice, a visually engaging infographic, and an 'interactive' format which asked a quiz question and then 'revealed' the correct answer in an infographic. We found seeing *any* type of cyber security advice strengthened SMB's intentions to update software and back up data, by nine per cent and six per cent respectively, compared to those who saw no advice. The interactive advice also appeared to improve SMB's accuracy in identifying phishing (fake) emails from genuine ones. However, in most cases plain text advice performed just as well as the same content presented in an infographic or interactive format. This suggests simple, jargon-free language may still be the most important aspect to consider in any advice.

To better understand which approaches resonate most with individuals, we conducted four focus groups across metropolitan and regional areas in New South Wales (two groups) and Victoria (two groups). We asked participants to tell us about their reactions to different design concepts, as well as talk to their level of cyber security expertise and their experience of cyber incidents.

Based on these findings, we designed advice using the *messenger effect* and tested the impact of our designs in an online survey experiment. We compared a 'peer' messenger to an 'expert' messenger (two senior government officials working in cyber security). We also tested whether participants responded more strongly to advice emphasising financial or non-financial costs of having poor cyber security.

We found some evidence messengers may have a small positive impact on people's intentions to update their software, but we only have moderate confidence in this finding. We also found no effect from messengers on people's intentions to use strong and different passwords across important accounts, and no effect on either cyber security practice from using different financial or non-financial loss framing. Overall, our research suggests making cyber security advice salient and engaging can help make key messages stand out. However, simply providing advice alone is insufficient to change behaviour, and further research is needed to better understand which formats, framing, and channels are most impactful for different groups.

Why?

As more aspects of people's lives and businesses become digitised and connected online, the risks of poor cyber security intensify

Increasingly, online attackers aim to breach the information security systems of businesses and organisations to access the personal data of customers, suppliers, and staff members, ranging anywhere from people's email addresses to bank details and sensitive medical information. Between July and December 2019, there were 537 notifiable data breaches[1] reported to the Office of the Australian Information Commissioner, 43 per cent of which were due to malicious cyber incidents such as malware and 'phishing' emails (OAIC 2020)[2]. This doesn't account for the number of smaller-scale incidents experienced by small businesses and individuals in their personal lives, of which the ACSC receives an average of 148 reports per day.

Not only is the scale of cyber incidents increasing, so too is the level of sophistication. Although many people are aware of 'phishing'[3] (or scam) emails and know to avoid clicking on suspicious hyperlinks or attachments, they may be less familiar with 'spear phishing' emails, which embed relevant information (such as colleagues' names or an individual's personal details, which may themselves be stolen) to be more convincing. Attacks like these threaten individuals in their personal lives, as well as businesses and large organisations such as banks, government agencies, and companies providing critical infrastructure.

It can be difficult to keep up-to-date with the latest cyber security advice

Although many people have a general awareness or knowledge of cyber security problems, they often have less knowledge of specific threats (Asgharpour et al. 2007). Given the evolving nature of cybercrime, it is unsurprising people find it difficult to keep up with the latest cyber security advice and threats, even when they intend to do so. For example, a study by the Australian Institute of Criminology on online consumer fraud found the majority of scam victims had tried to research the supposed company or individual before falling victim, but many were unable to distinguish between fake and legitimate websites (Emami et al. 2019).

[1] A 'data breach' is the term for when personal information held by an organisation is accessed without the permission of the organisation or person whose information is accessed. Under the Notifiable Data Breaches (NDB) scheme any organisation or agency covered by *The Privacy Act 1988* must notify affected individuals and the Office of the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved.

[2] For more information on different types of cyber incidents, see https://www.cyber.gov.au

[3] A phishing email is a fake email used by cybercriminals to get important personal or business information or to plant a virus in the reader's computer or mobile phone. The phishing email is often crafted to look like a genuine email from a real person or organisation, asking the reader to click on a hyperlink, open an attachment, or respond with critical details which the cybercriminal uses to impersonate the reader or access important accounts such as a bank account.

Providing a credible source of information is vital to tackling misperceptions

Many everyday users and small business owners are interested in cyber security advice, but it can be difficult to know which sources to trust, especially when there are real or perceived commercial interests on the part of the person or company providing the advice (e.g. laptop or mobile phone companies who may suggest their products are more secure than their competitors). As a result, people often encounter incidental sources of cyber security information through news articles and the advice of family and friends. These sources, however, are less likely to equip people with the knowledge they need to respond to potential threats (Rader & Wash, 2015).

Government websites act as an authoritative source of advice and resources for people and businesses seeking to understand cyber security

Websites providing clear, actionable, user-oriented information are important when people actively search for advice on cyber security (Rader & Wash, 2015). Governments act as an impartial, reliable, and authoritative source of this advice, and are best placed to inform people about the wide variety of attacks they could be subject to and protective measures they can adopt. Increasingly, governments around the world are striving to bolster their online presence to deliver this information to the public, including comprehensive websites in Australia, the UK, and New Zealand. Ensuring these websites are easy to find and navigate, and have compelling and engaging advice and resources for all users, is essential to bolstering their impact. Behavioural insights can offer tools to help.

What we did

Behavioural insights can help make cyber security advice easier to understand and adopt

We identified key cyber security practices people need most, and applied behavioural insights to make the advice about these practices stand out

We worked with the ACSC to identify some of the most common and important cyber security practices for individuals and small businesses. These were:

- creating strong and different passwords across important online accounts (such as online bank, email, and social media accounts),
- updating software as soon as there is a prompt to do so,
- backing up data, and
- being alert to the characteristics of phishing emails (scam emails seeking to embed a virus, or gain personal information or even money from the recipient by pretending to be someone they know, or a company they work with or buy from).

Although many people are familiar with these cyber security practices, our research and work with focus groups suggests people may be less familiar with the practical ways in which these practices protect them. Instead, what many people think of are the *friction costs*[4] associated with remembering multiple complex passwords (and often needing to reset these if they've been forgotten), being prompted to update software or back up data in the middle of a task, or losing legitimate emails to spam folders.

Without being reminded of the importance of all of these practices, it's easy to see how many people prefer to reuse passwords on multiple accounts, 'snooze' prompts to update software or back up data, and click past warnings about downloading attachments or clicking links in emails. To tackle these habits, we used behavioural insights to highlight the necessity and effectiveness of simple cyber security practices and challenge people's perceptions about the difficulty and value in enacting basic cyber security advice.

We designed different approaches to the same cyber security advice, and tested what worked with individuals and small businesses

To make advice interesting, memorable, and relatable for everyday people and small businesses owners, we applied different behavioural insights concepts to cyber security advice, and tested their impact in focus groups and two survey experiments. Specifically, we

[4] Friction costs are any barrier, however small, to a person beginning or completing an action. For example, requiring people to seek out additional information to make a decision, complete a form, or make an appointment are friction costs and can be the difference between someone following through with an action, intention, or decision, or not. See Kling et al (2012).

designed advice for everyday people applying cyber security advice in their personal lives, and small business owners (or operators with a role in key decisions for the business).

We chose these cohorts because both have limited time and expertise, and need timely, simple, and jargon-free advice. Like individuals, small businesses rarely have immediate access to IT support or comprehensive cyber security advice, as opposed to larger organisations and companies with dedicated teams and high-tech protection systems. We modified the same advice on key cyber security behaviours applicable to both groups to understand how differences in presentation and framing affect people's intentions to enact the advice in their personal lives or small business. See Table 1 for more details.

Table 1: Cyber security and behavioural insights concepts used in testing

	Individuals	Small businesses
Cyber security concepts	• ***Update software*** regularly, and especially ***when prompted***	
	• Use strong and different ***passwords*** across accounts	• ***Back up data*** regularly • Beware of ***phishing emails*** and avoid clicking on suspicious hyperlinks and attachments
Behavioural insights concepts	• ***Messenger effect*** of advice from either a 'peer' (another everyday user) or an 'expert' (someone from the cyber security field) • ***Framing*** of potential losses, making ***salient*** the possibility of financial or non-financial consequences (e.g. stress, time, or personal effects such as photos and files)	• Making ***salient*** the different advice by creating infographics to explain each concept. Additionally, using an interactive format to make the advice memorable by testing people's knowledge before showing them the advice • Reinforce a sense of responsibility and ***altruism*** by reminding businesses of how they can help protect the data of their customers and suppliers
Method	Online survey with an embedded experiment	Online survey with an embedded experiment
Sample	4,489 participants	1,186 participants

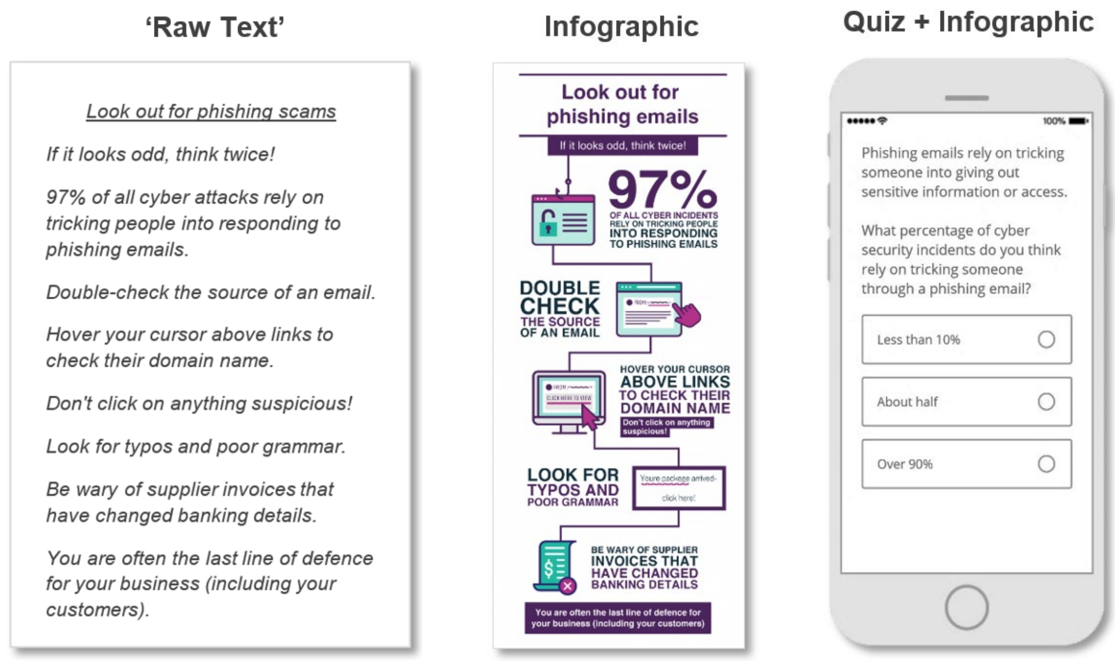
Applying behavioural insights to cyber security advice for small businesses

Making advice memorable and easy to interpret can help important information stand out for busy small businesses with other priorities and limited time

Many of us have numerous and competing demands on our time, energy, and attention, in both our personal and work lives. This *scarcity* can lead many people and small business owners, even those who strive to implement good cyber security, to forget, delay, or avoid implementing good practices. Additionally, the sheer volume of available information can lead to *information overload*, leaving many people to feel overwhelmed by different sources of advice on an already complex topic. To cut through the 'noise' of information individuals and small businesses encounter every day, cyber security advice must be engaging, easy to understand and apply, and relevant to their needs.

We hypothesised presenting cyber security information in a visually engaging way would make the advice stand out, and prompt small business owners and operators to implement new or improved cyber security practices based on our advice. We focused on three simple (but critical) cyber security behaviours for small businesses: keeping software up to date, backing up important data, and being wary of phishing emails.

We tested the advice in three ways: as plain text, as a visually engaging infographic, and in an 'interactive' format where participants were asked a quiz question about the cyber security topic first, and shown the answer using the infographic (see Figure 1).



'Raw Text'

Look out for phishing scams

If it looks odd, think twice!

97% of all cyber attacks rely on tricking people into responding to phishing emails.

Double-check the source of an email.

Hover your cursor above links to check their domain name.

Don't click on anything suspicious!

Look for typos and poor grammar.

Be wary of supplier invoices that have changed banking details.

You are often the last line of defence for your business (including your customers).

Infographic

Look out for phishing emails

If it looks odd, think twice!

97% OF ALL CYBER INCIDENTS RELY ON TRICKING PEOPLE INTO RESPONDING TO PHISHING EMAILS

DOUBLE CHECK THE SOURCE OF AN EMAIL

HOVER YOUR CURSOR ABOVE LINKS TO CHECK THEIR DOMAIN NAME

Don't click on anything suspicious!

LOOK FOR TYPOS AND POOR GRAMMAR

Youre package arrived- click here!

BE WARY OF SUPPLIER INVOICES THAT HAVE CHANGED BANKING DETAILS

You are often the last line of defence for your business (including your customers)

Quiz + Infographic

Phishing emails rely on tricking someone into giving out sensitive information or access.

What percentage of cyber security incidents do you think rely on tricking someone through a phishing email?

Less than 10% ○

About half ○

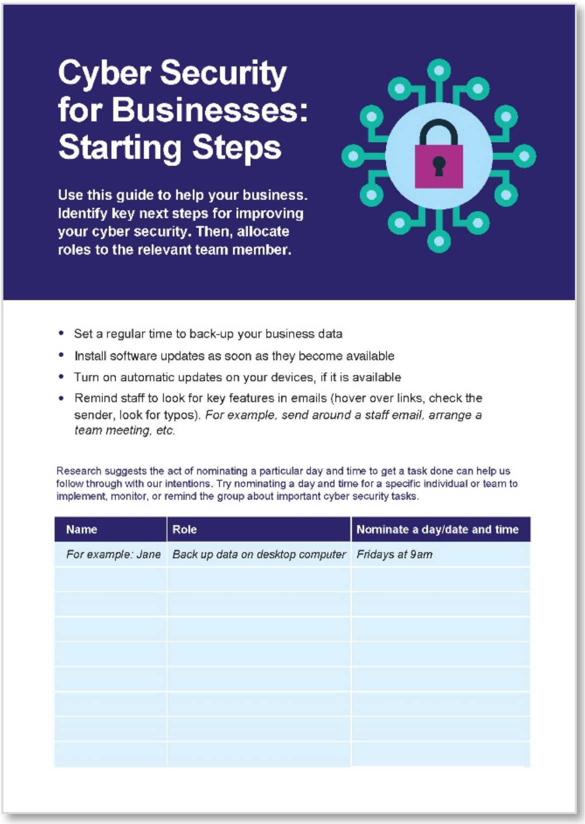
Over 90% ○

Figure 1: The control group saw no advice, while intervention groups were shown either plain text, an infographic, or asked a quiz question and shown the answer in the infographic format

1. We crafted a **plain text** version of the advice. The advice was simple, easy to read, and incorporated clear instructions on cyber security behaviours. We were careful to avoid jargon and technical terms to ensure the advice would be easily understood.

2. Drawing inspiration from the public health sector, especially the infographics of the World Health Organisation and other institutions, we designed three **infographic presentations** of cyber security advice (see Figure 1). The infographics incorporated simple language to reduce the complexity of cyber security jargon, and used icons and a narrative structure to make the advice more engaging. We also reinforced a sense of responsibility and *altruism* by emphasising how enacting the steps in the advice can help small business owners and staff protect not only their business, but also their customers, clients, and suppliers whose personal information they may store or have access to.
3. Finally, we designed an **interactive (quiz) format**, where participants were asked a question about the topic first, and then shown the infographic followed by an indication of whether their answer was correct. We thought asking people to first consider the problem before showing them more information about it would make the advice more *salient*, especially if the answer was surprising. For example, the fact 97 per cent of cyber incidents are the result of people clicking on hyperlinks or attachments in fake emails is much higher than most people expected, makes this fact stand out. Being surprised may lead some people to reconsider how much they think they know about cyber security and prompt them to want to know more.

We designed a checklist to help embed cyber security advice in day-to-day activities of small businesses



Cyber Security for Businesses: Starting Steps

Use this guide to help your business. Identify key next steps for improving your cyber security. Then, allocate roles to the relevant team member.

- Set a regular time to back-up your business data
- Install software updates as soon as they become available
- Turn on automatic updates on your devices, if it is available
- Remind staff to look for key features in emails (hover over links, check the sender, look for typos). *For example, send around a staff email, arrange a team meeting, etc.*

Research suggests the act of nominating a particular day and time to get a task done can help us follow through with our intentions. Try nominating a day and time for a specific individual or team to implement, monitor, or remind the group about important cyber security tasks.

Name	Role	Nominate a day/date and time
For example: Jane	*Back up data on desktop computer*	*Fridays at 9am*

To help business owners enact cyber security advice, we developed a ‘Starting Steps’ guide serving as both a *reminder* and a *commitment device*. Behavioural insights suggests people are more likely to implement a behaviour if they have written down a specific day and time to do it, and nominated a specific person to whom the task relates (Milkman et al 2013).

By assigning roles and days/times to implement actions, a checklist ensures behaviours can be made routine where they might otherwise be postponed or forgotten. The guide reiterated the advice provided in the plain text and infographics, and provided a blank checklist for business owners to fill in and embed those practices in their business.

Box 1: Behavioural insights concepts

Altruism is the desire to do or give something for the benefit of others (Andreoni 1990).

Commitment devices are actions, policies, programs enabling people to pre-commit to a goal or outcome. By committing a future self to an action, people are often more likely to follow-through, especially if the commitment defaults the future self to, for example, save more money (Cialdini 2008).

Information overload is the effect of having too much material or detail, often creating too many choices or decisions about which information is most important or relevant. Provided with too many options, people can often make sub-optimal decisions (Simon, H. A. 1969; Cherbnev et al 2015).

Loss framing draws on the findings from **loss aversion**, which is the tendency for people to behave differently when facing a loss compared to a gain of the same amount; people much prefer avoiding losses than making gains (Tversky & Kahneman 1991).

The messenger effect is the impact of a particular person or organisation, acting as the source of information, on how the information is received (Behavioural Insights Team 2010).

Scarcity or **cognitive overload** is a lack 'mental bandwidth'. We have limits on our cognitive resources, time, and energy, especially when we are busy or have few resources. Scarcity can mean we have less time or effort to make decisions well (or to make them at all). It can also amplify the effects of other cognitive biases (Mullainathan & Shafir 2013).

Reminders can come in a number of forms (letter, SMS, email, etc.) and can be personalised or generic. Numerous studies in different fields support the use of reminders to help people follow through with appointments, tasks, or actions (Clazolari 2014; Busso et al 2015; Karlan et al 2016).

Saliency is the effect of making something stand out or become more prominent (Taylor & Fiske 1979; Allcott & Wozny 2014; Castelo et al 2015).

Applying behavioural insights to cyber security advice for individuals

Using a messenger can make advice more personable and legitimate

Maintaining good cyber security practices can be especially difficult due to changing threats and risk mitigation strategies. This makes the authority and authenticity of the source or messenger delivering the advice all the more important. We know from other studies in behavioural insights the *messenger effect* can boost the impact of communications (Behavioural Insights Team 2010). In cyber security, the messenger is likely to be particularly important for increasing trust in the expertise, authority, and intent of the advice.

We used a government crest, and photos and stories from different messengers to make advice more authentic

To better understand which approaches resonate most with regular, non-expert users, we conducted four focus groups across metropolitan and regional areas in New South Wales (two groups) and Victoria (two groups) (see the Technical Appendix). We asked participants to tell us about their reactions to some different design concepts, as well as talk to their level of cyber security expertise and any experiences they may have had with cyber security incidents.

People in the focus groups responded well to both the sense of impartial authority provided by the Commonwealth crest, and advice delivered ‘from’ a peer messenger, whose everyday advice in the form of a personal story felt relatable. Based on these findings, we designed advice using the *messenger effect* and compared a peer messenger to an expert messenger (two senior government officials working in cyber security).

We also framed the consequences of inaction differently by highlighting potential financial or non-financial costs

We know many people are *loss averse*, meaning they can be more motivated to avoid losing money than they may be to gain it (Tversky & Kahneman 1991). Many people who are the victim of cyber incidents can lose money (sometimes substantial amounts), but they may also lose files, photos, or other non-monetary items which may still be very valuable to them. We designed two different approaches to the consequences of poor cybersecurity highlighting either financial or non-financial costs to see whether either framing was particularly impactful.

Example: Messengers – advice on using strong and different passwords

Plain text (no messenger)

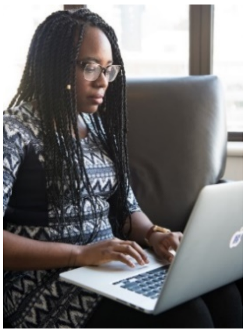
Setting strong passwords for your accounts online is important, the same way that locking your front door is when you leave home.

Last year in Australia, victims of hacking reported losing an average of $9,700. Hackers regularly get access both directly and indirectly to bank accounts because people have weak passwords or reuse them across different accounts online. Once someone has a password from one site, they can use that password (or try variations of it) to attempt to hack into other, more important accounts. Police don’t recover funds that are stolen online.

Don’t pay for weak passwords! Here’s what to do:

- Turn on two-factor authentication for your important accounts, such as a code sent to your mobile, for an extra layer of security.
- Use strong passwords on your accounts. A strong password is a passphrase of at least 13 characters, made up of about four words that are meaningful for you but not easy for others to guess. For example, ‘horsecupstarshoe’.
- Don’t use the same password on any of your accounts.
- Consider using a reputable password manager. It does the work so you don’t have to!

Peer messenger (passwords example)



Christina
Graphic Designer, Melbourne

Setting strong passwords for your accounts is important, the same way that locking your front door is when you leave home.

"I used to use the same password for almost everything. At most, I'd change the number at the end. Then, one of my passwords was stolen in a data breach. Because I had weak passwords and reused them across accounts online, hackers were able to guess my passwords by testing variations of another password of mine and got into my bank accounts. I lost $9,700."

Learn from Christina. Here's what to do:

- Turn on two-factor authentication for your important accounts, such as a code sent to your mobile, for an extra layer of security.
- Use strong passwords on your accounts. A strong password is a passphrase of at least 13 characters, made up of about four words that are meaningful for you but not easy for others to guess. For example, 'horsecupstarshoe'.
- Don't use the same password on any of your accounts.
- Consider using a reputable password manager.

It does the work so you don't have to!

Expert messenger (passwords example)

Karl Hanmore
Acting Head
Australian Cyber Security Centre

Setting strong passwords for your accounts is important, the same way that locking your front door is when you leave home.

"Many people don't realise how vulnerable having weak passwords or reusing them across accounts makes them online. Once someone has a password from one site, they can use that password (or try variations of it) to attempt to hack into other, more important accounts. In 2019, victims of hacking reported losing an average of $9,700. Many didn't realise that police don't recover funds that are stolen online."

Here's Karl's advice for protecting yourself online:

- Turn on two-factor authentication for your important accounts, such as a code sent to your mobile, for an extra layer of security.
- Use strong passwords on your accounts. A strong password is a passphrase of at least 13 characters, made up of about four words that are meaningful for you but not easy for others to guess. For example, 'horsecupstarshoe'.
- Don't use the same password on any of your accounts.
- Consider using a reputable password manager.

It does the work so you don't have to!

Survey participants were shown advice in either 'plain text' form with no messenger, or in 'peer' messenger or 'expert' messenger form. Participants saw advice on two topics (using strong and different passwords, and updating software) and were randomly assigned to a different form for each. We used two different peer and expert messengers for the different cyber topics.

Example: Financial and non-financial framing on the risks of not updating software

Financial loss

We’re all busy, so it can be hard to do the things we know are important for our online security. Although small steps like software updates can feel inconvenient at the time, the long-term prevention benefits can be huge.

Are your devices updated? Last year in Australia, victims of malware and ransomware reported losing an average of almost $3,000. Programs and apps can have flaws in their security that only get fixed when you update the software. If your phone or computer isn’t up-to-date, hackers can take advantages of these virtual “gaps” in your system to lock you out of your device, hold files or photos for ransom, or even use your device to commit crimes without you knowing. Older software like Microsoft Windows 7 is especially vulnerable.

Make sure your computers, phones, and tablets have the latest security:

- Turn on automatic updates on your devices, including your phone.
- When a pop-up message from a trusted application requests an update, accept it when possible.
- If you need to delay, set a reminder for yourself so you can update your device overnight or at a more convenient time.

Non-financial loss

We’re all busy, so it can be hard to do the things we know are important for our online security. Although small steps like software updates can feel inconvenient at the time, the long-term prevention benefits can be huge.

Are your devices updated? Last year in Australia, 4,359 people reported being victims of malware or ransomware. Programs and apps can have flaws in their security that only get fixed when you update the software. If your phone or computer isn’t up-to-date, , hackers can take advantages of these virtual “gaps” in your system to lock you out of your device, hold files or photos for ransom, or even use your device to commit crimes without you knowing. Older software like Microsoft Windows 7 is especially vulnerable.

Make sure your computers, phones, and tablets have the latest security:

- Turn on automatic updates on your devices, including your phone.
- When a pop-up message from a trusted application requests an update, accept it when possible.
- If you need to delay, set a reminder for yourself so you can update your device overnight or at a more convenient time.

In addition to seeing different messengers, advice was framed in terms of either financial or non-financial losses.

What we found

In short

- Simple, instructive advice increased small business owner’s intentions to improve their business’ cyber security. Seeing infographic or text formats of advice led ten per cent more business owners to say they would update their software, and six per cent more to say they would back up their data.
- We found different messengers did not make a difference to people’s intentions to improve their cyber security.
- People find government a trustworthy source, but for most people it’s not their primary source of cyber security advice.

Small businesses

Using engaging and interactive formats can make advice more impactful for some small business owners and operators

In our survey experiment involving small and medium business (SMB) owners and operators, we used behavioural insights to design clear, instructive, and jargon-free cyber security advice. We found the advice strengthened people’s intentions to implement the recommended cyber safety practices (keeping software up to date, backing up important data, and being wary of phishing emails) in their business. In particular, seeing infographic or text formats of advice led ten per cent more business owners to say they would update their software, and six per cent more to say they would back up their data (see Figure 2).

We also found providing advice in an interactive (quiz) format appeared to be effective in helping business owners correctly identify phishing and genuine emails in our phishing email quiz. For business operators who saw the interactive format, the average quiz score was 74 per cent, compared to 69-71 per cent for the other groups.

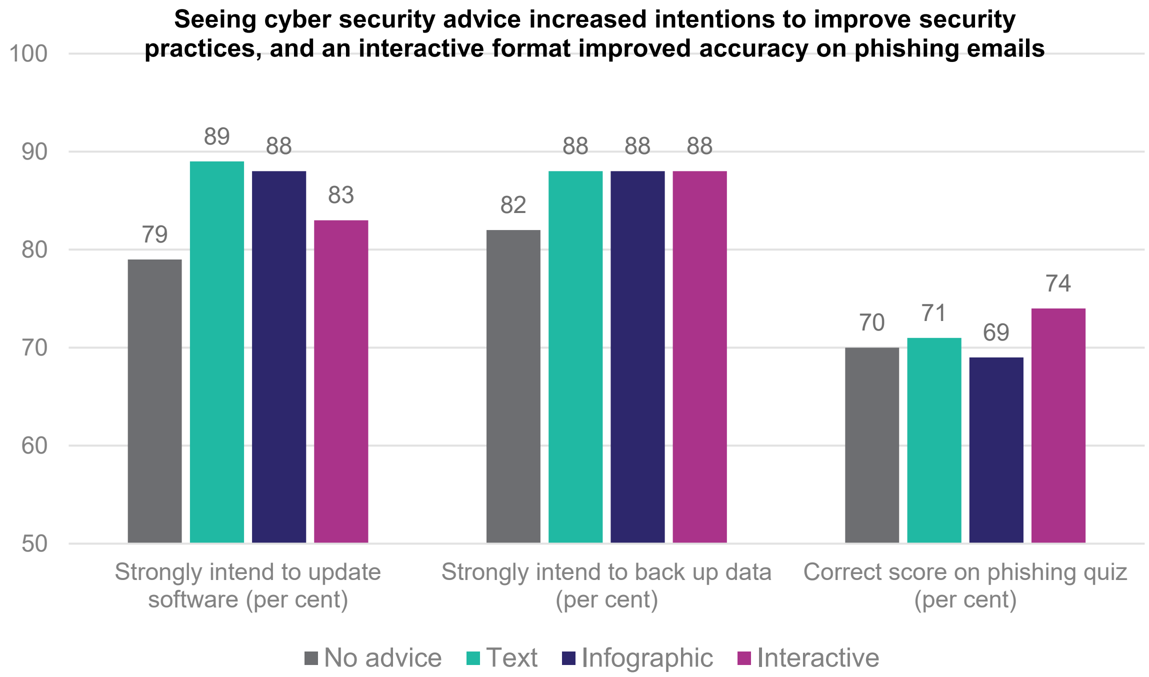


Figure 2: Seeing cyber security advice prompted small business owners to consider improving their practices. On the phishing quiz, interactive advice improved more people's ability to correctly identify phishing emails.

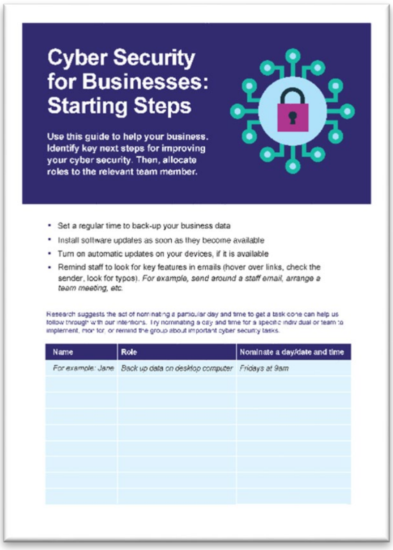
Different cyber security concepts may benefit from different formats, including plain text written in simple, jargon-free language

We think the success of the interactive group in correctly identifying phishing emails may be due in part to the fact an interactive format prompted participants to consider a cyber security topic before being shown a surprising or interesting fact. In the interactive format, we found most business owners *incorrectly* answered a question about the proportion of cyber incidents resulting from phishing emails. Having been surprised to learn they may not know as much about phishing emails as they thought they did, our participants in the interactive group may have been more attentive to the email examples in our quiz than participants in other groups.

Advice on well-worn topics such as phishing emails, which many people believe they know well, could be most effectively presented in a quiz format. By challenging their overconfidence, a quiz may prompt people to pay closer attention to the related advice.

However, it is also notable the plain text equivalent of the advice on software updates and backing up data performed just as well as a visually engaging infographic. Although we were surprised the more colourful and interesting version of the advice did not have a greater impact than plain text, this finding reflects the fundamental importance of clear, compelling, and jargon-free advice, whatever the topic.

Business owners and operators are drawn to resources to help them apply cyber security advice in practice



Cyber Security for Businesses: Starting Steps

Use this guide to help your business. Identify key next steps for improving your cyber security. Then, allocate roles to the relevant team member.

- Set a regular time to back-up your business data
- Install software updates as soon as they become available
- Turn on automatic updates on your devices, if it is available
- Remind staff to look for key features in emails (hover over links, check the sender, look for typos). *For example, send around a staff email, arrange a team meeting, etc.*

Research suggests the act of nominating a particular day and time to get a task done can help us follow through with our intentions. Try nominating a day and time for a specific individual or team to implement, monitor, or remind the group about important cyber security tasks.

Name	Role	Nominate a day/date and time
For example: Jane	*Back up data on desktop computer*	*Fridays at 9am*

> *"Reaffirmed actions already being completed as appropriate"*

> *"Clear information presented in a way that was easy to share"*

> *"As our bulk of backups are automatic I pinned the guide up in my office to remind me to double check that the backups were up to date"*

> *"All of the advice and tips were useful - and reminded me to implement most, if not all of them asap"*

~survey respondents

In a follow-up survey, we asked participants from our survey of SMB owners and operators whether they remembered the checklist we offered at the end of the first survey, and if so, whether they downloaded and used it. Of those who responded to our follow up survey, most remembered the checklist (79 per cent) and more than half had downloaded it (54 per cent).

We found 70 per cent of SMB owners and operators who used the checklist said they found it helpful. For some, it was a positive reaffirmation of their existing security practices. For others, it was a useful management tool for ensuring different staff members take responsibility for cyber security practices affecting the whole business. This suggests resources to help translate advice into action may be most effective in ensuring cyber security advice has an impact on people's daily habits, both in their business and personal lives.

Tools like checklists, reminders, and other mechanisms for personalising advice and making it relevant for individual needs may be more effective than simply highlighting the value of these practices. Although we did not test the effect of the checklist in our study, we believe this could be an area for further research.

Individuals

Overall, we found neither the messenger nor different framing of consequences increased people's intentions to enact the cyber security advice

In our survey with individuals, we found some evidence to suggest seeing advice from a messenger group (a peer messenger or expert messenger, as opposed to advice with no personal story attached) increased participants' intentions to update software. However, these effects were small, and we found no evidence to suggest the messengers increased intentions to create strong and different passwords. We also found little difference in outcomes between groups who saw advice describing financial losses compared to those with advice on non-financial losses. Overall, these results suggest simply providing advice is not enough to change people's practices.

It is possible our stylised advice with photos of messengers was too long or dense for most readers, or our choice of messengers were not impactful. As with the findings from the small business survey, this suggests the format of advice on more widely understood cyber security concepts (like passwords and updates) could benefit from a different approach (for example, a quiz or interactive format to challenge people's perceptions). It's also possible people may have benefited from a checklist or other resource they could download and make their own, as with the business owners and operators in our small business survey who we offered a 'starting steps guide' to assign roles and tasks to team members.

People find the government trustworthy, but it isn't their main source of cyber security advice

We found many participants in our individual survey said they turn to both government and peers for cyber security advice (Figure 3). In particular, 'government' (15 per cent) and 'friends and family' (17 per cent) were some of the top responses after 'internet security software companies' (23 per cent). Notably, different age groups found some sources of advice more compelling than others. For example, more participants who were 18-34 years old reported finding 'friends and family' and 'online sources' trustworthy sources of advice, compared with those 55 and older who overwhelmingly preferred 'internet security software companies' and 'government'.

This suggests government websites and other channels for advice could benefit from tailoring advice not only for the specific cyber security topic (as discussed above) but also for the audience. Older people may be more inclined to look for government websites or other resources for advice, whereas younger people may be more likely to view advice shared through their social circles, for example on social media.

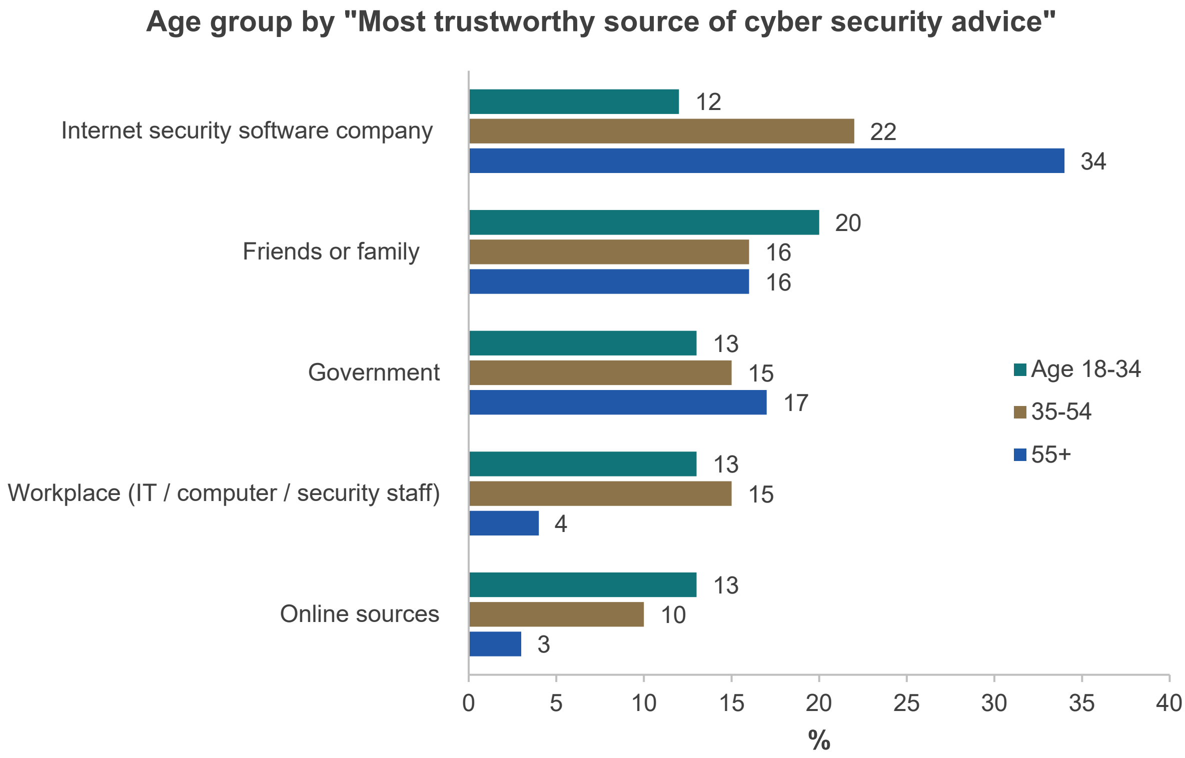


Figure 3: While the Government is a trusted source of information for around 15 per cent of Australians surveyed, internet security companies remain the dominant trusted source of information (23 per cent) followed closely by friends or family (17 per cent). Some response categories were omitted if they were below 10 per cent and not related to IT.

Discussion & conclusion

More research is needed to find the most effective formats and channels of advice for individuals and small business

Although some of our behavioural concepts had reasonable impacts on intentions and knowledge, we weren't able to demonstrate a consistently strong effect from any one format of advice. Additionally, respondents to our small business survey may not be representative of small businesses generally. For example, it's possible our survey attracted small business owners and operators already interested in cyber security, or those with more initiative. Consequently, changes in the presentation of advice may have a different impact for these business owners as compared to the broader business owner population.

Conversely, in our survey of individuals, we were able to recruit a national representative sample, meaning our results are more readily generalisable. The results from this survey may be more reflective of the Australian population in general because we had a balance of people from different age groups, genders, and location (by state) and did not rely on people volunteering their time.

Both our small business and individual survey experiments were somewhat removed from the 'real world'. For example, the experience of seeking out and reading cyber security advice on a government website is likely to be different to reading it in the context of completing a survey. Also we focused on respondents' stated intentions, which are less realistic than if we were to observe what they click on, download, or do on an actual website with cyber security advice, let alone whether they actually implement the cyber security practices.

One benefit of providing cyber security advice via websites and other online channels like social media is the ability to see how many people visit the site, click on links, and download or share resources. Further research could use A/B testing and other evaluation methods to see which formats of advice are most popular, and among which cohorts. This would provide a more accurate picture of how people actually engage with advice, and more in-depth research should seek to observe whether and how people enact this advice in their daily lives and work.

Applying behavioural insights to cyber security advice can help it stand out, but information alone may be insufficient to improve cyber security practices

We found simple, behaviourally-informed approaches to advice can help key messages about cyber security become more noticeable. In particular, some of our findings for businesses suggest more familiar cyber security concepts, such as being wary of links in suspicious phishing emails, can benefit from more engaging and distinctive formats. However, we also found more stylised designs were no more effective than plain text.

While this perhaps speaks to the power of providing simple, jargon-free advice, our results may also indicate information alone is not the only or even the most effective way to improve people’s cyber security practices. Our research with focus groups and surveys found many people and small businesses are either overwhelmed with other priorities, believe they have sufficient protections already, or don’t know where to start. Simply telling them to change their practices when they are already busy, uninterested, or overconfident, may not translate into actual behaviour.

Additionally, our research indicated a proportion of individuals and small business owners/operators in our surveys didn’t intend to perform *any* of the basic cyber security practices we asked them about. For some security practices, as many as 40 per cent of respondents expressed little to no intention to implement the practice in their personal or work life. This is despite seeing clear, engaging, and urgent advice about both the benefits and efficacy of these actions and the substantial consequences of inaction. It’s possible these people already do everything our advice suggested. It’s also possible some are still unconvinced by the advice, or are pessimistic about their likelihood of following through with it.

Thankfully, the internet and technology industry is increasing the degree to which cyber security practices are automated, so users have less to worry about and less to enact themselves. For example, Apple’s latest iPhone releases have built on the existing automatic updates setting and introduced this as the default setting to ensure users have maximum security measures through updated software, with minimal interruption (updates occur overnight from 2am) and no effort on the part of the user (Singh 2020). Our findings support the increased use of default settings in this way. Given the changing nature of threats, the limited time and expertise of users, and the increasing sophistication of cybercriminals, the industry providing the devices and software where these activities take place must strive to make it as easy as possible for regular people to stay safe digitally and online. Greater coverage and less reliance on proactive behaviour from regular individuals and small businesses will benefit everyone, including the experts trying to protect them.

References

Allcott, H., & Wozny, N. (2014). Gasoline prices, fuel economy, and the energy paradox. *Review of Economics and Statistics*, 96(5), 779-795.

Andreoni, J. (1990). Impure altruism and donations to public goods: A theory of warm-glow giving. *The Economic Journal*, 100(401), 464-477.

Asgharpour, F., Liu, D., & Camp, L.J. (2007). Mental Models of Computer Security Risks. *WEIS*.

Behavioural Insights Team (BIT) (2010), *MINDSPACE Report*, Available at:

https://www.bi.team/publications/mindspace/

Busso, M., Cristia, J., Humpage, S. (2015), Did you get your shots? Experimental evidence on the role of reminders, *Journal of Health Economics*, 44:C, 226-237

Castelo, N., Hardy, E., House, J., Mazar, N., Tsai, C., & Zhao, M. (2015). Moving citizens online: Using salience & message framing to motivate behavior change. *Behavioral Science & Policy*, 1(2), pp. 57–68.

Chernev, A., Böckenholt, U., & Goodman, J. (2015). Choice overload: A conceptual review and meta-analysis. *Journal of Consumer Psychology*, 25(2), 333-358.

Cialdini, R.B. (2008). *Influence: Science and Practice*, 5th ed. Boston: Pearson.

Emami, C., Smith, R. G., & Jorna, P., *Online fraud victimisation in Australia: Risks and protective factors, Australian Institute of Criminology*, AIC Research Report 16. 2019.

Karlan, D. & McConnell, M., Mullainathan S. & Zinman, J. 2016. Getting to the Top of Mind: How Reminders Increase Saving, *Management Science*, INFORMS, vol. 62(12), 3393-3411.

Kling, J. R., Mullainathan, S., Shafir, E., Vermeulen, L. C., & Wrobel, M. V. (2012). Comparison friction: Experimental evidence from Medicare drug plans. *The quarterly journal of economics*, 127(1), 199-235.

Milkman, K. L., Beshears, J., Choi, J. J., Laibson, D., & Madrian, B. C. (2013). Planning prompts as a means of increasing preventive screening rates. *Preventive Medicine*, *56*(1), 92-93.

Mullainathan, S. & Shafir, E. (2013), *Scarcity: Why Having Too Little Means So Much*, Henry Holt and Company.

Office of the Australian Information Commissioner (2020), *Notifiable Data Breaches Report: July–December 2019*, available at:

https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-databreaches-statistics/notifiable-data-breaches-report-july-december-2019/

Rader, E. & Walsh, R. (2015), Identifying patterns in informal sources of security information, *Journal of Cybersecurity*, 1:1, 121–144. Simon, H. A. (1969). Designing organizations for an information-rich world. *Brookings Institute Lecture*.

Singh, J (2020), “iOS 13.6, iPadOS 13.6 Released With Auto Updates Over Wi-Fi Setting: How to Download”, *Gadgets360*, 16 July, https://gadgets.ndtv.com/mobiles/news/ios-13-6-ipados-update-download-new-features-changes-apple-2263834

Taylor, S. E., & Fiske, S. T. (1975). Point of view and perceptions of causality. *Journal of Personality and Social Psychology*, 32(3), 439–445

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference-dependent model. *The quarterly journal of economics*, *106*(4), 1039-1061.

© Commonwealth of Australia 2020

ISBN 978-1-925364-44-6 password123: applying behavioural insights to cyber security advice

Copyright Notice

Third party copyright

Attribution

This publication should be attributed as follows: Commonwealth of Australia, Department of the Prime Minister and Cabinet, password123: *Applying behavioural insights to cyber security advice.*

Use of the Coat of Arms

Australian Government

BETA

Behavioural Economics Team
of the Australian Government

General enquiries beta@pmc.gov.au

Media enquiries media@pmc.gov.au

Find out more https://behaviouraleconomics.pmc.gov.au/