Australian Government
Department of the Prime Minister and Cabinet

BETA

After the crime

Experiences of cyber security incidents

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 [this report];**
- password123: Applying behavioural insights to cyber security advice.

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

Since the launch of ReportCyber on 1 July 2019, there have been 59,806 cybercrime reports at an average of 164 per day or approximately one report every ten minutes (ACSC, 2020). Some of the most commonly reported incidents in 2019 were scams such as phishing emails. People also reported more serious incidents like identity theft, online fraud, online romance scams, and business wire fraud (ACSC, 2019). Many more incidents are likely to go unreported, particularly if victims feel ashamed of what happened or are unsure of whether to report, meaning the total number of incidents in Australia is likely to be much higher.

To better understand how and why people become the victim of cyber incidents, BETA dedicated a section of our research on cyber security (including focus groups, two surveys, and analysis of feedback on the ReportCyber tool) to the topic of experiencing a cyber incident.[1] Our participants included everyday users – individuals who do not work in IT or related fields – and small business owners and operators. Like individuals, small businesses face an evolving cyber landscape without the protections of dedicated teams or specialist software many larger organisations can afford.

We found more than half (60 per cent) of our survey participants had experienced some kind of cyber incident in the previous twelve months; for most, this involved a criminal 'scam,' attempting to steal money or information. We also found experiencing a cyber incident was related to age and self-rated cyber security expertise. For example, younger people (aged 18-34) reported experiencing more cyber incidents, and more serious incidents (such as identity theft and online image abuse) than older people did. Younger people also reported more 'fatalistic' attitudes, believing incidents would happen again and were unavoidable.

Like younger people, many small businesses who had experienced an incident perceived future incidents as inevitable. Businesses who had *not* experienced a cyber incident generally considered it 'possible' they could experience an incident in the next 12 months, while those who had were more likely to consider a future incident as 'almost certain'.

Based on these findings, cyber security advice would be most impactful if it were tailored according to several factors: individual's level of cyber security awareness, their time spent online and the type of activities they engage in, and their perceptions about their ability to change their practices. All of these factors are influenced by expertise and age.

Of those who reported the incident to authorities, most people were motivated by a desire to help protect others from experiencing a similar incident. Based on this finding, drawing on people's sense of altruism could be an effective way of encouraging more people to report cyber incidents to authorities. Once people report, there is a valuable opportunity to provide cyber security advice to help improve their cyber security and avoid future incidents.

[1] For more on the broader piece of research see our report, password123: *Applying behavioural insights to cyber security advice*, or for more technical details see the Technical Appendix.

Why?

Every day, the government receives around 150 reports of an online or digital incident[2]

Since the launch of ReportCyber on 1st July 2019, there have been 59,806 cybercrime reports at an average of 164 per day or approximately one report every 10 minutes (ACSC, 2020). While this is a decrease from the previous year (with 64,567 reports in the 12 months prior), the volume of reported cybercrimes remains immense. Cyber incidents can range from catchall scams like a phishing[3] email sent to thousands of email addresses, to personal and targeted attacks on specific individuals. The most common cyber incidents in 2019 were identity theft, online romance scams, and business wire fraud[4] (ACSC, 2019). Many more incidents go unreported, particularly if victims are unsure of what to do or feel ashamed of what happened, meaning the total number of cyber incidents in Australia is likely to be much higher.

In addition to the stress and time taken to recover from a cyber incident, the financial costs of cyber incidents can be immense. In 2019, the reported financial losses to cybercrime were $328 million (ACSC, 2019). Scams such as phishing emails, fake websites, or callers pretending to be from a real company or government, are one of the most common cyber incidents and can be especially costly. The Australian Competition and Consumer Commission's (ACCC) Scamwatch found losses from scams in 2019 totalled over $140 million (ACCC, 2020). This represents a 57 per cent increase in reported losses from scams since 2017.

People who have experienced an incident are in a timely position to improve their cyber security practices and avoid being re-victimised

Experiencing a cyber incident can motivate some people to improve their cyber security practices, but for others it can be paralysing. In one study, researchers found people who recognise a threat but feel powerless to protect themselves are more likely to respond to the threat with fear and 'learned helplessness' (Bada & Nurse, 2020). To counter this, it is critical to strengthen people's belief in the effectiveness of cyber security practices and their own ability to implement them. For example, the same research found people who had more 'self-efficacy' (an individual's perception of their capacity to control the environment around them) were also more flexible and adaptable when faced with threats or challenges (Bada & Nurse,

[2] This represents the combined figures of incidents reported to the ACSC from July-September 2019 and to the ACCC in 2019.

[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.

[4] For more explanations of the different types of cyber incidents, visit https://www.cyber.gov.au.

2020). Victims of fraud and other online incidents can take measures to avoid becoming a victim again in the future, but they must feel empowered in their ability to do so.

Experiencing a cyber incident can be stressful and costly, so it is important the process of reporting an incident is straightforward and reassuring

Although not every report of a cyber incident will result in further investigation (e.g. because the perpetrator is overseas or unidentifiable), the details of every report can build a better picture of the cyber incident landscape for authorities, in turn helping authorities to disrupt cybercrime. It is important that those who experience a cyber incident are willing and able to report details to the relevant authorities and through the right channels. There are a number of established reporting channels online, such as ReportCyber, Scamwatch, and the Office of the eSafety Commissioner. The easier and simpler these online forms can be to locate and complete, the more likely victims are to report an incident in the first place and complete the form in full. This data can then provide valuable insights for authorities, and the reporting process itself can be a timely opportunity to provide victims with advice, next steps, and improve their cyber security going forward.

Behavioural science

Experiencing a cyber incident can change people's perspectives and subsequent behaviour to cyber security

People take action if they believe they can protect themselves from a threat – and they take the threat seriously

Like preventative health, good cyber security is measured through the *absence* of an event or incident. This makes it difficult to observe and be motivated by the consequences of having good cyber security practices. Originally developed to explain adherence to healthy behaviours in public health, Protection Motivation Theory explains how people respond cognitively when they encounter a threat (Rogers 1975, 1983) (see Box 1).

There have been numerous applications of Protection Motivation Theory to cyber security behaviour[5]. In one such study, researchers found the more participants believed their actions can help protect their personal computers, the more likely they were to use and update antivirus software (Dodel & Mesch 2017).

Based on Protection Motivation Theory, if a person believes the threat of a cyber security incident is minor, they are unlikely to change or adapt their behaviour digitally or online. However, even if a person believes the threat is severe, they too may not change their behaviour if they believe there is nothing they personally can do to mitigate it. Two conditions are needed for people to take action – if they believe a threat is serious and they believe they can address it, they probably will.

Box 1: Components of Protection Motivation Theory

Threat appraisal

- **Severity:** how severe does a person perceive the threat as being?
- **Vulnerability:** how much does the person perceive themselves to be personally at risk?

Coping appraisal

- **Efficacy:** how effective do they believe the recommended action or behaviour is at mitigating the threat?
- **Self-efficacy:** how much do they believe they can personally follow through with the required action or behaviour?

[5] See Workman et al., 2008; Anderson and Agarwal, 2010; Shillair et al., 2015; Boehmer et al., 2015; Youn, 2005; Johnston & Warkentin, 2010; Ifinedo, 2012; Siponen et al., 2014.

People's decisions are affected by the attitudes and practices (real or perceived) of the people around them

In addition to perceptions of their own ability to keep up good cyber security practices, people's actions are also affected by the behaviour of those in their social circle. For example, we found many participants in our focus groups on cyber security cited their friends, colleagues, and family members (including teenage children) as being a source of information about online and digital security (BETA 2020, see also the Technical Appendix). Seeing or perceiving others to be following good cyber security practices can be a strong motivator for many of us, as *social norms* often play an important role in our decision-making (Shultz et al 2007; Sherif 1936). This effect can be both positive and negative. If people believe others do little or nothing to protect themselves online, they may be less inclined to change their own behaviours.

Thinking about others is a strong motivator for change, even if the behaviour can also help protect ourselves

For those who do not believe they are personally at risk, but believe the risk exists, it may be more impactful to reinforce how having good (or weak) cyber security can affect others, especially people they know and care about. We know *altruism* can be a powerful motivator for people, and this applies in cyber security as well. In our focus groups, many participants said they were motivated to protect their businesses and family from cyber incidents (BETA 2020, see also the Technical Appendix). This was particularly common for parents, who cited protecting their children from cyber incidents as a primary motivator. These insights were supported by findings from our online survey, where respondents who said they had experienced a cyber incident explained their main motivation for reporting the incident was to prevent the incident from happening to others (BETA 2020, see also the Technical Appendix).

People's actions are also affected by the amount of time, effort, and resources they have available

Even for people who intend to keep up their cyber security as best they can, many can find themselves with limited time and energy to follow through with these intentions. We all have limited 'mental bandwidth' with which to make decisions each day, and in times of high stress this can lead to mental *scarcity* (the effect of having too little time or energy to make decisions well – or to make decisions at all). Those who are experiencing scarcity or *cognitive overload* are likely to be at high risk of delaying or avoiding making necessary changes to their cyber security practices if this involves some costs in effort and time. For this reason, cyber security advice must be as easy and efficient as possible to implement.

Box 2: Behavioural insights concepts

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).

Social norms are the social rules that people pay attention to in order to know how to behave in a given context or situation (Sherif 1936).

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

What we found

In short:

- Sixty per cent of people we surveyed had experienced some type of cyber incident within the last 12 months alone, the most common of which was a scam (affecting 51 per cent).
- Younger people reported experiencing a greater number and variety of cyber incidents. Excluding scams, which are common across all age groups, 36 per cent of younger people reported experiencing one or more different types of incident in the last 12 months compared to 21 per cent of people aged 35 and over.
- Altruism is a powerful motivator for reporting an incident.
- Better understanding of cyber security and being more active online may also improve people's ability to recognise and classify cyber incidents.

We conducted research on cyber security, and included specific questions to learn more about the experience of a cyber incident

We conducted focus groups and two online survey experiments to design and test the effect of different formats of cyber security advice. In the qualitative components of this research, we also asked participants whether they had experienced a cyber incident and if so, whether and how it affected their cyber security behaviour afterwards. Here, we outline notable findings about the experience of victims from these three studies, primarily drawing on the two surveys. One survey had a nationally representative sample of 4,489 individuals; the other was a survey of 1,186 small-to-medium business operators. Many of the findings from the surveys support findings from the focus groups, which had a smaller sample of 30 participants from urban and regional areas in New South Wales and Victoria, balanced by age and gender.[6]

People with better cyber expertise may report more cyber incidents

We asked our survey respondents to rate their level of expertise in online and digital security, ranging from 'nothing' or 'very little' to 'a lot'. Interestingly, those who stated they had 'a lot' of expertise in online and digital security also reported experiencing more cyber security incidents (see Figure 1). It is possible some people may be overconfident in their cyber security abilities: overestimating their knowledge and leaving themselves open to more cyber incidents.

[6] For more information on these studies, see Technical Appendix, or read the password123: Applying Behavioural Insights to Cyber Security Advice, BETA 2020.

It is also possible more expertise simply means better reporting. Some of the more sophisticated cybercrimes (such as malware) can be difficult to detect, and determining the correct cyber security term to describe it can be equally difficult.[7] This sentiment was reflected in some of the focus group discussions, with participants reflecting on the difference between more 'visible' incidents in the physical world and more 'hidden' ones online, as well as the complex terminology to describe incidents. To add to this, the process of experiencing a cyber incident itself may subsequently result in an increase in actual and/or self-reported expertise.

*"If someone breaks into your house you know it has been broken into – **with cyber security you may well not know** until a lot of damage has been done"*

- focus group participant

*"**Things have evolved so much** since I was a kid at school….I've tried to [stay] in the loop with all this stuff but it's still a bit foreign to me"*

- focus group participant

The ability to detect and put a name to a cyber incident may partly explain why the number of people who have experienced a "scam" is more evenly spread across different levels of understanding, and so much more frequently reported than other incidents (Figure 1). Even those with little to no understanding may feel more confident in their awareness of scams and the terminology to describe them, compared to jargon such as "malware" or "image abuse". People who have a better understanding of different types of cyber incidents may therefore report more of these incidents, and a greater variety of incidents, because they are better at detecting and classifying them.

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

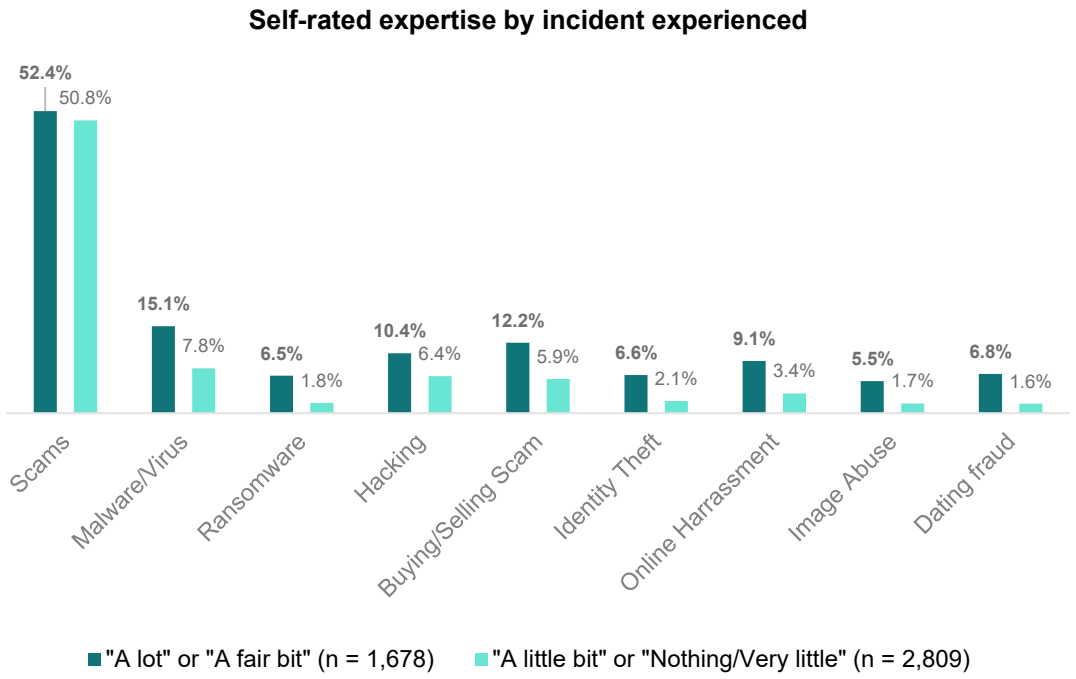

Figure 1: Experience of cyber incidents within the last 12 months, disaggregated by self-reported cyber security expertise level

Younger people reported a great number and variety of cyber incidents, but their beliefs about the inevitability of cyber incidents should be challenged

Our survey found most people (51 per cent) had seen or experienced an online scam in the last 12 months. Although experiences with scams were even across all age groups, younger people reported experiencing a greater variety of other, more serious cyber security incidents, such as identity theft, harassment, and online image abuse (see Figure 2).

A proportion of young people may become victims because they are overconfident in their abilities or more inclined to take risks. For example, more young people (50 per cent) described themselves as having 'a lot' or 'a fair bit' of expertise, compared to over 35s, (32 per cent).

> *"I think **old[er] people are just ignorant [about] what can actually happen** in today's day. Before it might [have been] really easy to hack into your computer… these days I think it's more [common to experience] hacking into your profile to steal your identity."*
>
> *- focus group participant*

Young people also admitted engaging in more risky activities than older people, such as clicking email links from unknown senders (37 per cent, compared to 19 per cent of people aged 35 or older) and using public Wi-Fi for banking (38 per cent, compared to 13 per cent of people aged 35 or older).

We also found younger people tended to be more fatalistic about cyber security. Far fewer young people strongly agreed with the statements "it is important to reduce the chance of cybercrime happening to me", "it is important to protect my personal details online", and "I can take actions to reduce the chance of cybercrime happening to me". If younger people feel a cyber incident is 'inevitable' and any efforts to protect themselves are unlikely to work, advice for younger people should reinforce how

effective basic cyber security practices are. Challenging people's beliefs about the effectiveness of having good cyber security measures could be effective in encouraging better practices among groups who falsely believe there is nothing they can do.

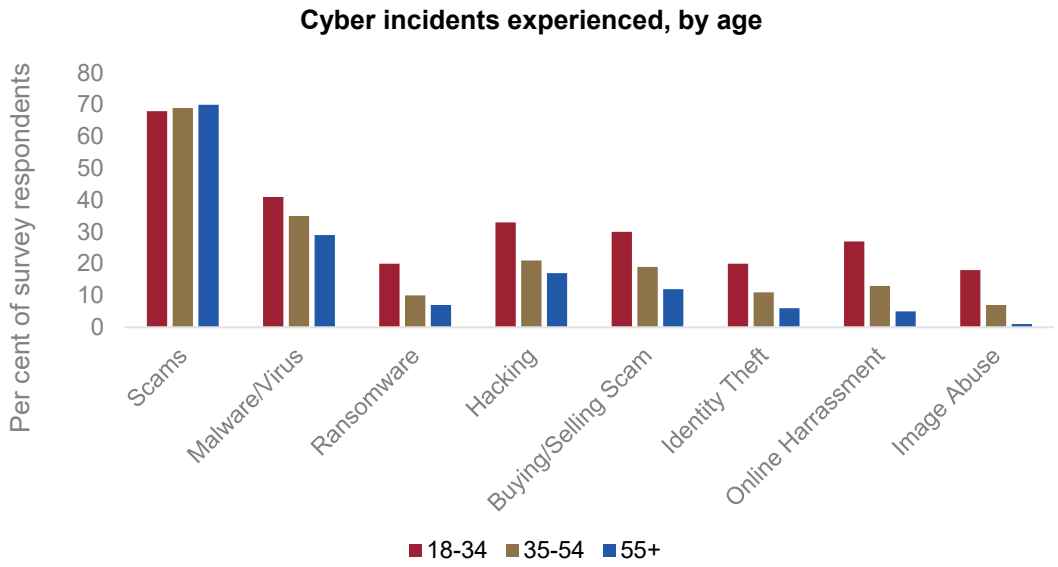

Figure 2: Most survey respondents who said they had experienced a cyber incident reported experiencing a scam, but younger people consistently reported more experiences of other incidents

As with better expertise, younger people in our survey may also report experiencing more cyber incidents, and a greater variety of incidents, because they can better identify when something has happened and report it using the relevant cyber security terminology. Many younger people have grown up with online and digital forums and devices, and may have more understanding of how to navigate these. Additionally, younger people may also experience more cyber incidents because they are more active online or digitally. It is possible fewer older people said they engaged in risky online behaviours because they spend less time and do fewer activities (such as banking) online or digitally (e.g. through the use of mobile phone applications). It may also be the case that their inexperience online makes it more difficult for them to identify risks and report having experienced them.

Small businesses face similar barriers to individuals

The majority (nearly 98 per cent) of small and medium enterprises (SMEs) in Australia have fewer than 20 employees. Of these, 62 per cent are sole traders, and 27 per cent are micro-businesses with fewer than five employees (Australian Small Business and Family Enterprise Ombudsman 2019). Similar to their personal lives, most sole traders and micro-businesses do not have access to dedicated or expert IT support, meaning responsibility for cyber security falls to staff who are also maintaining day-to-day operations.

Our survey of SME owners and operators supported this, with 97 per cent of sole traders managing IT security themselves. Although small and medium business were somewhat more likely to outsource IT security than sole traders, a majority still managed cyber security themselves. As with everyday individuals, participants in our SME survey reported cyber security practices had to compete with other demands associated with running a business for time and resources. Understandably, many SMEs felt they were not always able to keep up-to-date with the latest cyber security advice and practices.

> *"I still need to update my website so it is more secure.* ***Finding time*** *to deal with IT issues is hard when you run a small business and need to work a lot of hours"*
>
> *- SME survey respondent*

> *"[Our] system [was] hacked and…locked down. [The data] back up had not been working and was unsupervised, and much data was lost.* ***Hard in [a] medical practice!"***
>
> *- SME survey respondent*

Also like individuals, experiencing a cyber security incident affected business' understanding of cyber security and their perception of risk and vulnerability. 62 per cent of participants in our survey reported experiencing a cyber incident. This experience changed their evaluation of risk dramatically: businesses who had not experienced a cyber incident generally considered it 'possible' that they could experience an incident in the next 12 months, those who had experienced an incident were more likely to consider a future incident as 'almost certain'. As with young people, there is a risk some business owners become fatalistic about experiencing an incident. Reinforcing the effectiveness of basic cyber security practices in businesses is vital, especially for those who have experienced a cyber incident in the past.

People are motivated to report a cyber incident to help protect others

In our survey of individuals, we asked survey respondents who said they reported a cyber incident what their main motivation was. We found nearly half (44 per cent) of respondents who had reported an incident did so to warn others (Figure 3). Altruism can be a powerful motivator, and these findings suggest more people could be encouraged to report cyber incidents if they are inspired to help others. In another study, BETA found encouraging people to share cyber security news and "pay it forward" to friends, family, or colleagues who could benefit, more than doubled the number of people who attempted to share (BETA 2020).

Altruism is already part of the ReportCyber reporting system, which thanks users for reporting and highlights how their report helps the Australian Government disrupt cybercrime and protect people like them. Simple messages like these can be the difference between someone choosing to report, providing a more detailed response, and considering other people they know who could benefit from advice to help prevent the same thing happening to them.

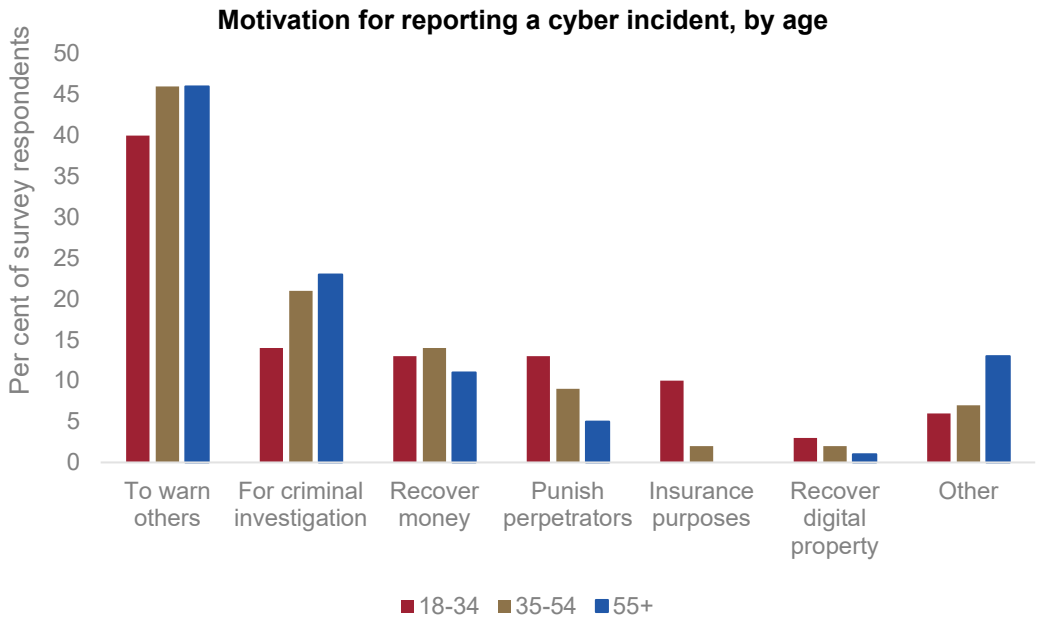

Figure 3: Victims' self-described reason for reporting, disaggregated by age bracket (n = 1,275)

Discussion & conclusion

Draw on people's sense of altruism to encourage more people to report

Our findings suggest people are motivated to help others avoid falling victim to the same cyber incident they have experienced. Drawing on this sense of altruism could be an effective way to encourage more people to report a cyber incident they might otherwise have kept to themselves. Our survey results support this, as do findings from another study on cyber security advice, in which a simple call to action to 'pay it forward' led to more than double the amount of sharing compared to the same information with no altruistic message (BETA 2020).

The more information available about emerging threats and trends, the better chance authorities have of understanding, identifying, and ultimately disrupting cyber incidents. Reporting is also a valuable opportunity for victims to get access to resources and support, and to learn what practices they can implement to avoid experiencing an incident again in the future.

Submitting a report is an opportunity to instil new and better practices

Cyber security advice aims to reduce the real and perceived barriers to having good cyber security, especially when someone has experienced an incident. Improving people's understanding of and ability to detect cyber incidents is important, but cyber security advice should also aim to improve people's belief they can contribute to their own protection, and reinforce how effective simple steps (such as updating software) can be.

Advice should vary depending on people's level of expertise and amount of time they spend online. Our findings suggest barriers facing SMEs are similar to those facing individuals. While the advice should be tailored to the needs of small business (especially around specific cyber incidents like business email compromise), advice should still be informed by behavioural models like Protection Motivation Theory, focusing on equipping people with the tools needed and the belief those tools will protect them.

Further research and testing is needed

Much of our data on people's experiences of cyber incidents came from self-report survey responses which, while providing interesting insight, covers only a small fraction of victim's experiences. Future research should further investigate how experiencing a cyber incident affects subsequent cyber security behaviours, and how best to support people in the event they become a victim.

It would be useful to understand when and how people report cyber incidents, and what can be done to further encourage people to provide details to authorities. Improving people's cyber vocabulary and understanding could help, but there also needs to be more effort to

reduce the degree of jargon and complexity in cyber security terminology. Together, we can reduce and prevent cyber incidents in Australia and work to disrupt cybercrime against everyday individuals and businesses.

References

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

Australian Competition and Consumer Commission (2020), Scam statistics, available at: https://www.scamwatch.gov.au/scam-statistics?scamid=all&date=2019.

Australian Cyber Security Centre (ACSC)(2020), *ACSC Annual Cyber Threat Report: July 2019 to June 2020.* Available at: https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Australian Small Business and Family Enterprise Ombudsman (2019), *Small Business Counts: Small business in the Australian economy - July 2019*, Commonwealth of Australia.

Anderson, C.L., Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q. 34 (3), 613–643.

Australian Cyber Security Centre, *Cybercrime in Australia – July to September 2019*. 2019.

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In Emerging Cyber Threats and Cognitive Vulnerabilities (pp. 73-92). Academic Press.

Boehmer, J., LaRose, R., Rifon, N.J., Alhabash, S., Cotten, S.R., 2015. Determinants of online safety behaviour: toward a strategy for public education. Behav. Inf. Technol.34 (10), 1022.

Behavioural Economics Team of the Australian Government (BETA), Department of the Prime Minister and Cabinet. (2020). *password123: Applying behavioural insights to cyber security advice.*

Dodel, M. & Mesch, G. (2017), "Cyber-victimization preventive behavior: A health belief model approach", Computers in Human Behavior 68 (2017) 359-367.

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.

Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31 (1), 83–95.

Johnston, A.C., Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS Q. 34 (3), 549–566.

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

Sherif, M. (1936). *The psychology of social norms*.

Shillair, R. & Dutton, W.H. (2016). Supporting a cybersecurity mindset: getting internet users into the cat and mouse game. Available at: http://dx.doi.org/10.2139/ssrn.2756736.

Schultz, P. W., Nolan, J. M., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2007). The constructive, destructive, and reconstructive power of social norms. Psychological science, 18(5), 429-434.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.

Workman, M., Bommer, W.H., Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Hum. Behav. 24 (6), 2799–2816

Youn, S., 2005. Teenagers' perceptions of online privacy and coping behaviors: a risk–-benefit appraisal approach. J. Broadcast. Electron. Media 49 (1), 86–110.

ISBN 978-1-925364-46-0 After the crime: experience of cyber security incidents

Australian Government

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/