Australian Government
Department of the Prime Minister and Cabinet

BETA

On the alert

Using behavioural insights to boost the impact of cyber security alerts

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

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.

Acknowledgements

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 4

Executive summary 5

Why? 6

What we did 7

What we found 10

Discussion & Conclusion 14

References 15

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 [this report];**
- After the crime: Experiences of cyber security incidents;
- 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

We partnered with the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) to find ways of boosting the impact of an email alert system. The ACSC alert service alert system (the 'alert service') is a free email subscription service available to the public. An alert is sent to subscribers whenever an emerging cyber security trend or threat becomes apparent. The alerts outline what people should look for, how to avoid or prevent the incident from happening to them, and what to do if someone may have been impacted. The alert service has been running since 2010 and had over 57,000 subscribers as of August 2020.

Despite the large reach of the alert system, email can be a difficult platform to spread awareness compared with other, more visible channels such as SMS or social media. We applied behavioural insights to the email design to bolster its effects, and tested these different design aspects using a randomised controlled trial. Our email trial was launched in February 2020, and used the top performing alerts of 2019 as the basis for the alert content. Subscribers were randomly assigned to receive an alert with one or more of our new design features (or a business-as-usual alert with the standard branding). Everyone received the same email content.

We trialled two new behaviourally informed design features: salient icons at the top of the page designed to give readers information about the urgency or action required at a glance, and a banner calling upon users to share the alert with their contacts.

We found including icons increased email open rates and interaction with the alert, and encouraging subscribers to share the alert with others increased forwarding rates. Without the icons, 2.9 per cent of subscribers interacted with the email by clicking on embedded links. This increased to 3.6 per cent for the best performing icon. Of those whose email did not include a sharing banner, 0.3 per cent shared the email by forwarding it or through social media. This more than doubled to 0.8 per cent of those whose email did include a banner.

Small improvements to emails can make a big difference when applied to the alert service database with over 57,000 subscribers. For example, adding an action icon to a business-as-usual alert could result in over 940 more readers opening the email. Including a sharing banner could result in around 320 more people sharing each alert with friends, family, and colleagues. Including a timing icon could result in an extra 360 people saving or printing a copy of the alert. Icons and banners are low-cost, low-effort ways to improve the spread and appeal of emails with important information for the public.

Why?

Cybercrime is on the rise. People need timely information and advice on immediate threats so they can protect themselves.

Each year cyber incidents are affecting more people

As people's business and personal lives are increasingly digitised and moved online, criminals seek to coerce or trick everyday users into sending money and sharing personal information. The consequences of these incidents can be substantial and long lasting. Between 1st July 2019 and 30th June 2020, the ACSC responded to 2,266 cyber security incidents and received 59,806 cybercrime reports at an average of 164 cybercrime reports per day, or one report every 10 minutes (ACSC, 2020). Cybercrime is one of the most pervasive threats facing Australia, and the most significant threat in terms of overall volume and impact to individuals and businesses. The Australian Competition and Consumer Commission's (ACCC) Targeting Scams 2019 report identified Australians lost over $634 million to scams in 2019 (ACCC, 2019 in ACSC, 2020). While the true cost of cybercrime to the Australian economy is difficult to quantify, industry estimates have previously placed cyber security incidents as high as $29 billion annually (ACSC, 2020).

Although many users are aware fake emails and websites exist, scams are increasingly more sophisticated; using logos and branding of real companies, reproducing real SMS conversations (such as legitimate text messages from Australia Post), and embedding relevant and true information into emails (such as colleagues' names or an individual's personal details, which may themselves be stolen). A study conducted by the Australian Institute of Criminology found the majority of scam victims tried to research the purported company or individual, but were unable to distinguish between false and legitimate websites (Emami et al., 2019).

The alert service helps keeps people in Australia informed about the latest threats

To help minimise the spread of cybercrime and keep people informed, the Australian Cyber Security Centre (ACSC) sends email notifications to alert users about new and emerging cyber threats. The ACSC alert system (hereinafter referred to as the 'alert service') notifies the reader about the incident, how to avoid falling victim, and next steps for those who may have already been affected. The alert service is free, and anyone can subscribe by signing up online with an email address. To date, the service has over 57,000 subscribers and has grown by over 5000 users each year for the past three years.

What we did

People are motivated to share urgent cyber security news with friends, family, and colleagues. We drew on people's sense of community and altruism to help increase awareness of incidents and encourage widespread behaviour change.

A lack of familiarity with cyber security incidents may lead some people to underestimate the prevalence and seriousness of such incidents

Cyber security is an emerging, changing, and complex topic affecting many people, and it can be difficult to translate awareness into action. Although common methods of cybercrime - such as phishing emails or scam text messages - are familiar to many users, some of the more sophisticated tools of cybercrime are less understood by most. While the experience of incidents such as ransomware (a computer virus used to hold a person's files 'hostage' unless a ransom is paid to the attackers) may be less common, the impact for individuals can be severe.

Some of the behavioural challenges in improving the cyber security of individuals can be linked to people's tendency to overestimate or underestimate the probability of events based on their experiences or beliefs. The *congruence bias* can lead us to underestimate the prevalence or chance of an event if we have not experienced it before or have no example from elsewhere for us to draw on (Wason, 1960). This occurs because we tend to look for confirming evidence for our opinions and worldviews, rather than consider alternative explanations. In cyber security, this means a lack of experience or exposure to the breadth, type, or seriousness of cybercrime could lead many everyday users to conclude these events are unlikely to happen to them, or are the result of their expertise and judgement rather than chance (ideas42, 2017).

Even if people are aware of cyber security threats, learning how to mitigate threats requires time, effort, and expertise

Even when people have a good sense of the risks of poor cyber security and strive to protect themselves, the rapidly evolving nature and sophistication of cybercrimes means it can be difficult to be aware of active threats (or even recognise them) and apply the latest advice. Moreover, many people have busy lives and competing priorities for their time and energy. Our *bounded rationality* means few, if any of us, have the ability to find, evaluate, and compare the sources of cyber security advice and apply these practices, let alone on a constant basis.

This, in addition to the plethora of websites, blogs, resources, and personal sources of information such as family, friends, and colleagues, can make it difficult for people to discern fact from fiction and maintain their awareness of the latest threats and advice. This *information overload* can lead people to avoid or delay making a decision altogether. To cut

through the noise, cyber security advice must be easy to understand and adopt, timely in its delivery, and stand out amongst the many other notifications and distractions of everyday life.

Box 1: Behavioural insights concepts

Congruence bias is the tendency to overrely on their initial hypothesis, and ignore alternative explanations or disconfirming evidence for an event or pattern (Wason, 1960).

Bounded rationality is the idea people have limits on their time, energy, and brainpower (Simon, 1982). It is an alternative concept to the idea of the 'rational actor' in economics, who is presumed to weigh up all choices and consider all information before making an informed, and optimal, decision.

Information overload is the effect of having an excess of information requiring our attention, which can lead us to make suboptimal decisions, or delay or avoid making decisions altogether (Simon, 1971).

We designed new icons to make it easier to quickly understand the urgency and type of action people need to take to avoid falling victim

The alert service sends timely email notifications when a new and widespread cyber security threat comes to the attention of the Australian Cyber Security Centre. Anyone can sign up to the service by subscribing online and providing an email address. Although the alert service has a relatively high email open rate (49 per cent on average for the last 10 alerts), alerts and other important information delivered via email is more easily ignored or missed by many people in comparison to other channels, such as SMS (BETA, 2019). To make the email alerts more salient and therefore more likely to be opened, interacted with, and shared, BETA designed a series of icons for the top of the emails (Figure 1). The icons aimed to make the email more attractive to the reader, and make the urgency of alert and the type of response required by the reader easier to quickly understand.

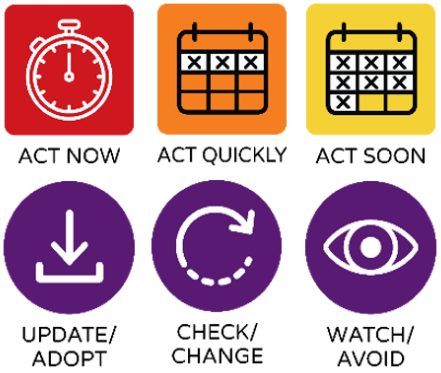

Figure 1: Icons designed for the alert service. We tested the timing icon for 'Act Quickly' and the action icon for 'Check/Change'.

To design a 'warning system' of icons for the alerts, we drew inspiration from common warning systems familiar to people in Australia, such as the bushfire wheel, and action-oriented rules-of-thumb like 'slip, slop, slap'. People like familiar concepts, and tend to feel more positively towards something if they have seen or heard of it before (Zajonc 1968). This is known as the *mere exposure effect*. Using icons drawing on familiar concepts in Australia and abroad (such as traffic light colours) makes them more readily interpreted.

People can also be a source of support for one another by sharing information and advice from trusted sources

We also suggested including a banner or button to encourage people to forward the alert and draw on their sense of *altruism* (Figure 2). Helping others can be a powerful motivator, at times even more motivating than doing something for personal gain or benefit (Andreoni 1990). One prominent example from a study by Grant and Hoffman (2011), found signs encouraging doctors to wash their hands in order to protect their patients were more effective at improving hand washing than signs encouraging doctors to protect themselves. This is echoed in findings from a survey BETA conducted of individuals, in which the most common motivator for reporting a cybercrime was to prevent it from happening to others (BETA, 2020).

Taking an altruistic approach to the alerts (and any communication about cyber security) can encourage people to consider others as well as themselves. The act of forwarding the message can reinforce the social aspect of cyber security practices ('it's everyone's responsibility'), increase the spread of information, and harness the fact many people turn to friends, family, and colleagues for information about cyber security. We designed a button with a call to action for readers to 'pay it forward' and consider others in their social circle who could benefit from knowing about the information in the alert.

Figure 2: We included a banner at the top of some of the email alerts encouraging people to consider sharing the alert with others

Box 2: Behavioural insights concepts in the designs

Mere exposure effect is the tendency for a person to prefer or feel more positively toward something if they have seen or heard of it before (Zajonc, 1968).

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

What we found

In short:

- A salient call to action (encouraging people to share the email) increased sharing rates.
- A salient icon at the top of the email (denoting either urgency or an action to be taken) increased interaction with email content, as well as the likelihood of opening the email and likelihood of saving a local copy of the contents.
- The benefits are modest, and come with negligible cost and risk.

We tested the effect of adding icons and banners to the alert service emails using a randomised controlled trial

To measure and compare the effect of including one of two icons and a sharing banner, alert service subscribers were randomly assigned into one of six email groups (Figure 3). The alert featured a summary of the 'top' alerts of 2019, as measured by open rates for alert emails sent the previous year. The emails were sent in February 2020, with data collected over a week-long period. For details of the trial design, refer to the Technical Appendix.

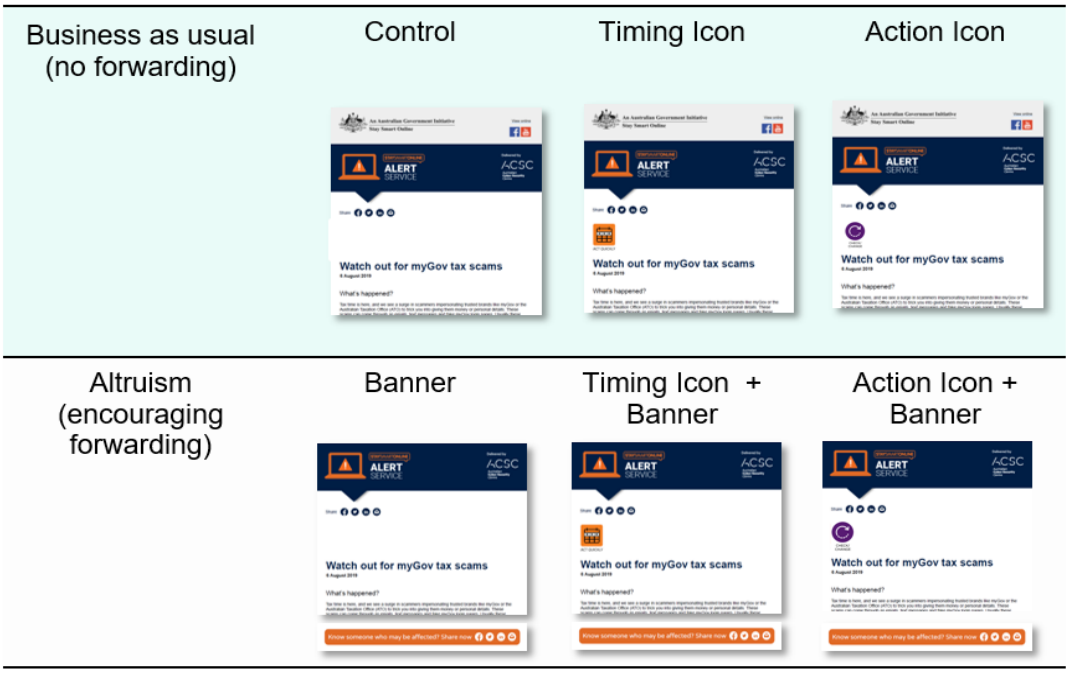

Figure 3: We used a factorial trial design to test both the use of icons, the use of a banner, and the combination of both.

A banner encouraging sharing significantly increased sharing rates

Those who received the sharing banner were more than twice as likely to share the email (see Figure 4). Sharing was measured by clicking on any of the social media links, a sharing button, or the hyperlink in the banner for those whose email included it. Although these figures appear modest, applied to the current subscriber base, including our banner could have led to around 320 more people sharing the alert.

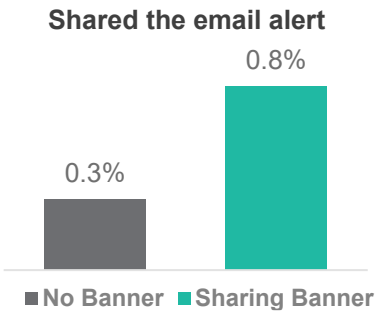

Figure 4: Number of individuals who shared the alert, split by whether the email included a sharing banner. See the Technical Appendix for details.

It is likely our results *underestimate* the amount of actual sharing behaviour. We were able to measure the number of readers who clicked on hyperlinks in the email, but had no information about what the reader did within their own email platform (for example, forwarding or printing the email using Outlook functions rather than the hyperlinks in the email itself).

The hyperlink in the sharing banner redirected readers to a page where they could manually enter email addresses they wished to send the alert to. While it allowed us to measure how many readers intended to forward the email, we acknowledge the extra burden of completing an online form may have led most people to opt for the convenience of using the forwarding function in their email platform. We weren't able to detect whether people forwarded the email using their email platform, so the sharing rate could be much higher than we were able to measure.

Including icons increased the amount readers interacted with the emails, and chose to print or save them

Compared to those whose email had no icon, the action and timing icons increased subscriber interaction by 11 per cent and 21 per cent respectively (Figure 5). We measured user interaction by the number of clicks on any of the hyperlinks in the email. For example, some hyperlinks in the body text of the email led to further information on the ACSC website (cyber.gov.au) about each of the 'top alerts' featured in the email. There were also links for each of the social media buttons (Facebook, Twitter, and LinkedIn) which allowed readers to share the alert directly on these platforms. Finally, we also had links to allow readers to forward the message on—separately from the sharing banner, which had its own hyperlink—and to print or save a copy of the alert.

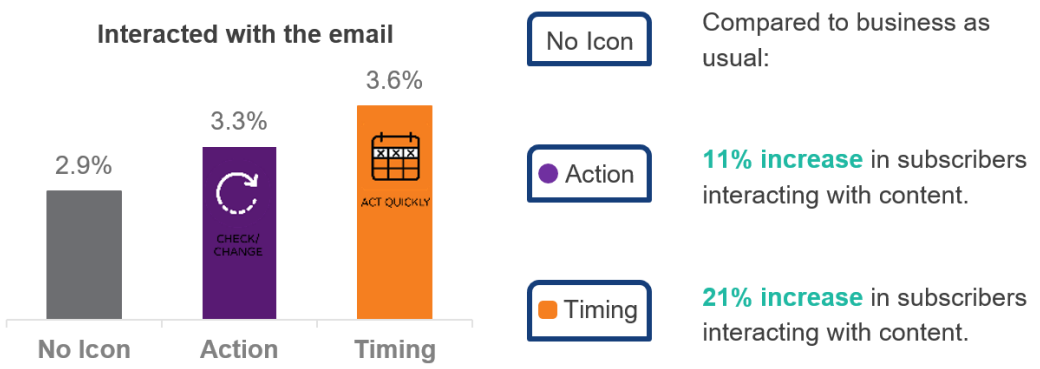

Figure 5: Rate of interaction with the email content for each variant of icon. A one percentage point difference equates to 570 people, based on 57,000 subscribers. The percent increase was calculated from values rounded to 2 decimal places.

We also found the icons had an effect on printing or saving the alert

Compared to emails with no icon, including either icon increased the rate of clicking on the 'print or save this email to pdf' hyperlink by around 65 per cent (Figure 6). Like the forwarding rates, we expect this could be an underestimate of the true rate of printing or saving the email, with many readers likely using the print or save functions in their email platforms rather than the link in the email itself.

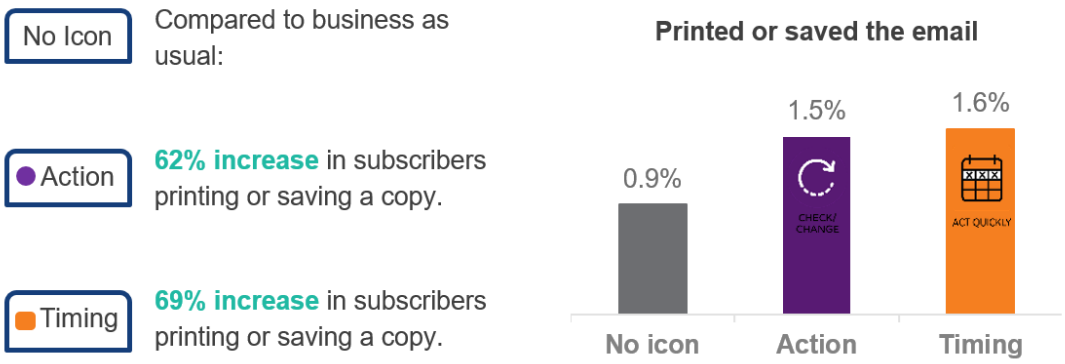

Figure 6: Rate of subscribers selecting option to print/save a copy of the email content for each variant of icon. A one percentage point difference equates to 570 people, based on 57,000 subscribers. The percent increase was calculated from values rounded to 2 decimal places.

Including icons also had a modest impact on email open rates

This may be because people preview emails through email clients (such as Outlook) without opening them fully, so seeing an icon at the top of the email in preview mode may have motivated readers to open the email fully. Of those whose email had no icon, 43.0 per cent opened the email. With icons, this raised to 44.6 per cent (action icon; an increase of 2%) and 43.9 per cent open rates (timing icon; an increase of 4%).

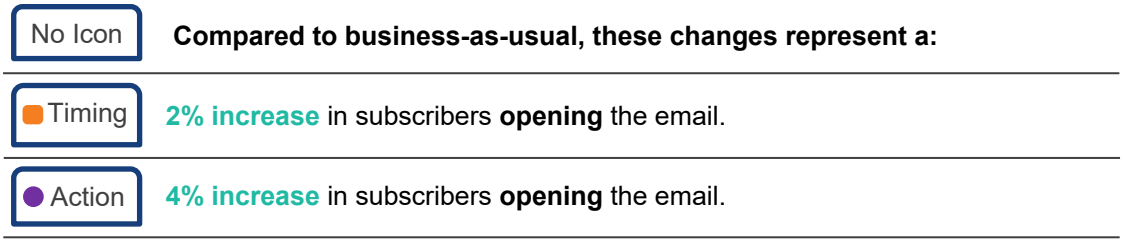

Figure 7: Rate of subscribers opening the email content for each variant of icon. A two percentage point difference equates to 1,140 people, assuming 57,000 subscribers.

Discussion & Conclusion

In the real world:

What do the results mean on a broader scale? If the effect sizes from the trial were applied as business-as-usual to the alert service with its subscriber base of approximately 57,000 readers:

- An action icon could result in around **940** more subscribers **opening** each alert.
- A sharing banner in the alert could result in around **320** more people **sharing** each alert with friends, family, and colleagues.
- A timing icon could result in an additional **350** people **interacting more deeply** with the content of each alert, and actively seeking more information – and around an extra **360** people saving a local copy.
- Based on the number of alerts sent out during 2019 (23) the addition of an action icon and sharing banner could have resulted in more than 7000 additional shares and more than 6000 additional people engaging deeply with the content.

The ACSC alert service plays a valuable role in providing timely advice on emerging cyber security threats to help everyday people avoid falling victim. As cyber threats continue to evolve and change, individuals benefit from receiving information and advice on how to identify, prevent, and mitigate emerging risks. With an already large subscriber base and high email open rates, the alert service is one example of how government agencies and other organisations can help spread the word on new threats targeting individuals, as well as provide general advice on how to improve and maintain cyber security in general.

Our research shows simple tools such as icons can increase opening and interaction rates in emails. Given the volume and variety of information – let alone cyber security advice – available via the internet today, useful and urgent advice such as the email alerts needs to stand out among other email traffic. Including easy-to-interpret icons drawing on common heuristics about urgency and risk, is a cost-effective and impactful way to circulate cyber security advice.

Readers themselves can act as an important catalyst for behaviour change among their social circles. Encouraging individuals to share information and advice about emerging threats is an effective tool for increasing awareness both of new cyber risks and of government services like the alert service. By directing family, friends, and colleagues to advice on a cyber security threat, we can also spread awareness about the government agencies and resources they can access to improve their cyber security practices, report incidents if they occur, and stay updated on the latest developments.

References

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

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

Baron, J., Beattie, J., & Hershey, J. C. (1988). Heuristics and biases in diagnostic reasoning: II. Congruence, information, and certainty. Organizational Behavior and Human Decision Processes, 42(1), 88-110.

Behavioural Economics Team of the Australian Government (2019), *Credit when it's due: reducing credit card debt*. Department of the Prime Minister and Cabinet.

Behavioural Insights Team (2013). 'Applying Behavioural Insights to Charitable Giving' Cabinet Office.

Blau, A., Alhadeff, A., Stern, M., Stinson, S., Wright, J (2017), Deep Thought: A Cyber Security Story, ideas 42, New York, USA.

Emami, C, Smith R G, Jorna, P (2019), *Online fraud victimisation in Australia: Risks and protective factors*, Australian Institute of Criminology, available at: https://www.aic.gov.au/publications/rr/rr16.

Grant, Adam & Hofmann, David. (2011). It's Not All About Me: Motivating Hand Hygiene Among Health Care Professionals by Focusing on Patients. Psychological science. 22.

Office of the Australian Information Commissioner (2019), *Notifiable Data Breaches Report: July–December 2019*, available at: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/.

Simon, H. (1971). Designing Organizations for an Information. Rich World. Speech at the Johns Hopkins University and Brookings Institution Symposium.

Simon, H. A. (1982). Models of bounded rationality. Cambridge, MA: MIT Press.

Wason, P. C. (1960). 'On the failure to eliminate hypotheses in a conceptual task'. Quarterly Journal of Experimental Psychology. 12 (3): 129–140.

Zajonc, R.B., 1968. 'Attitudinal effects of mere exposure.' Journal of personality and social psychology, 9(2p2), p.1.

ISBN 978-1-925364-45-3 On the alert: using behavioural insights to boost the impact of cyber security alerts

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/