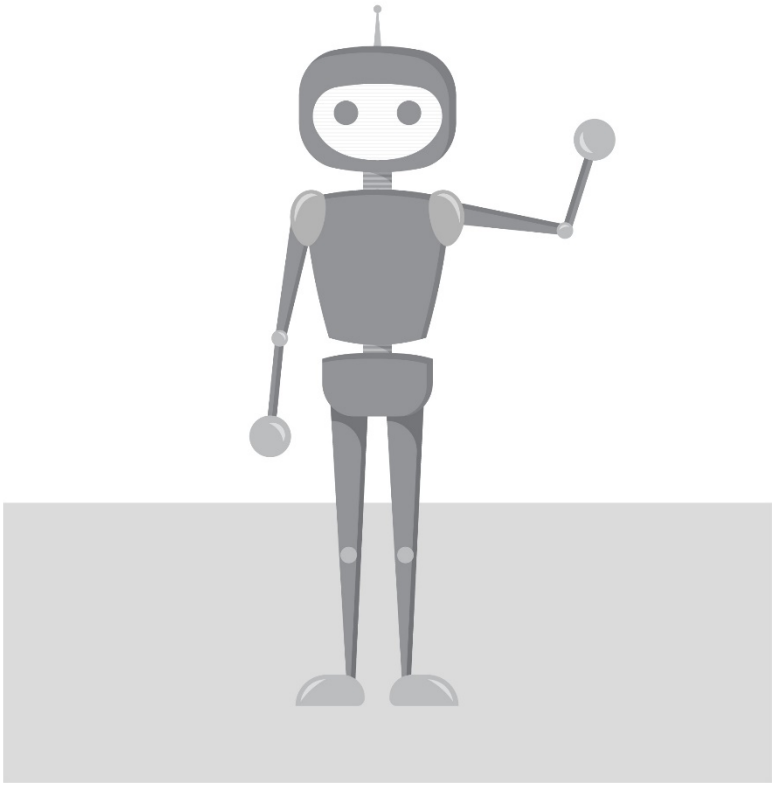
Australian Government
Department of the Prime Minister and Cabinet

BETA



Technical appendix:
evaluations in 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: Laura Bennetts Kneebone, Scott Copley, Andrew Bromwich, Harry Greenwell, Shea Houlihan, Michael Bleasdale, Hanne M Watkins, Ashley Breckenridge, 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 RCT 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 Technical Appendix provides the methodological and analytical spine for 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. In this Appendix, we present the experimental designs, interventions and results for each of the following projects:

- A trial designed to bolster the impact of an alert service to inform people of emerging cyber threats,
- A trial aiming to improve the saliency of cyber security advice for small businesses,
- A trial aiming to improve the saliency of cyber security advice for individuals.

The associated BETA reports which detail research findings correspond to the following sections of this Technical Appendix:

On the Alert describes how behavioural insights were used to boost the impact of emails in the Email alert service randomised controlled trial.

After the crime delves further into the experiences of those impacted by cyber security incidents, by looking at survey responses from the Cyber security survey for small and medium business and the Cyber security survey of individuals.

password123 highlights findings from the survey experiments that were conducted as part of the Cyber security survey for small and medium business and the Cyber security survey of individuals.

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

Email alert service randomised controlled trial

Technical details

Overview of the Stay Smart Online (SSO) Email Alert Service RCT

We conducted a randomised field experiment in partnership with the Australian Cyber Security Centre (ACSC), an Australian Government entity within the Australian Signals Directorate. The study sought to improve the Stay Smart Online (SSO) email alert service, (hereby referred to as the 'alert service') which informs users about the latest cyber threats and vulnerabilities within an Australian context and provides advice on how to address any risks to their devices or computer networks. Specifically, the study looked at the impact of various changes to the email content on engagement, click-through rates, and how often the emails were shared with others.

All subscribers to the alert service as of 19 February 2020 received an email outlining prominent online security threats from 2019. We used this retrospective content due to the impracticality and uncertainty of trialling interventions on a real alert, considering the various challenges already posed by delivering urgent, important advice.

We randomly assigned the 60,508 subscribers to receive one of six messages via email, where the unit of randomisation was individual subscribers to the alert service. The trial used a 2x3 factorial design. That is, we had two independent variables (IV):

- A 'call to action' IV with two levels (the inclusion of a 'sharing banner', or not),
- A 'heuristic icon' IV with three levels (the inclusion of an 'action icon', a 'timing icon', or no icon).

The ACSC sent the experimental emails to its subscriber base on 27 February 2020. Swift Digital manages the mailing platform for the ACSC and routinely collects data on email bounces, open rates, and whether subscribers click on any email links. We used this data to assess the impact of the treatments on open rates, interaction with the email (by clicking on links), and sharing the email (either by forwarding it or on social media). We downloaded this data one week after the emails were sent.

The project was approved through BETA's ethics approval process, with risk assessed in accordance with the guidelines outlined in the National Statement on Ethical Conduct in Human Research. It was reviewed by a delegate committee in accordance with the National Statement and was assessed as low risk.

Pre-registration and pre-analysis plans

We pre-registered this trial on both the American Economic Association RCT Registry (RCT ID no. AEARCTR-0005501) and the BETA website on 26 February 2020, before the trial had commenced. This pre-registration included an initial pre-analysis plan that detailed our proposed analysis, including our research hypotheses.

Since we had a very large data set (with around 60,000 participants initially), we pre-specified we would randomly select half of the data—the 'test data set'—for our initial analysis. Depending on the results of this analysis, we planned to update our pre-analysis plan, and then conduct further analysis on the 'holdout data set'.

We uploaded the updated pre-analysis plan to the AEA RCT registry on 8 April 2020, prior to any analysis being undertaken on the holdout data. Changes in the updated PAP are described below, along with one deviation from the updated plan. In the detailed results below, we report the results from both the test data and the holdout data.

Interventions

This study tested two sets of interventions: a 'call to action' and different 'heuristic icons'.

IV. A: Call to Action: Half of the recipients received an email with only the typical set of share buttons while the other half received a call to action—referred to henceforth as a 'sharing banner'—in the form of a salient banner calling upon readers to share the email for the benefit of others (Figure 1).

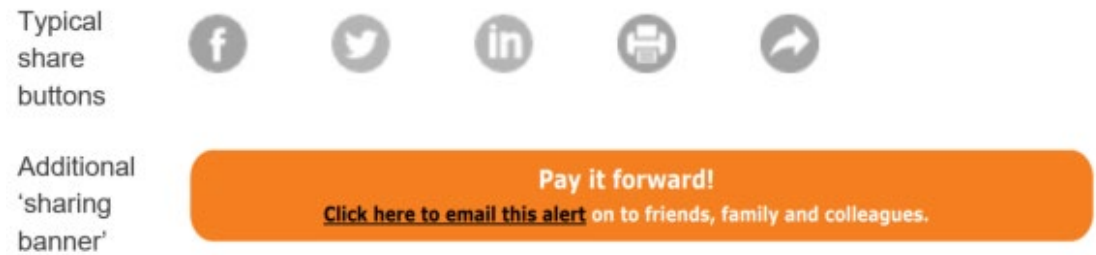


Figure 1: Call to action

IV. B: Heuristic Icons: Individuals received one of three possible emails with differing visual designs: a standard email, an email with an action icon, or an email with a timing icon (

). The final icons used in the trial were 'Check/Change' (action) and 'Act Quickly' (timing), as they were deemed most appropriate to the email's content.

Figure 2: Heuristic icons

The table below shows the notation used to refer to the individual groups formed from our two interventions (Table 1).

Table 1. Factorial design for the two interventions

		Heuristic icons		
		Standard (B0)	Timing icon (B1)	Action icon (B2)
Call to Action	**No sharing banner (A0)**	A0B0	A0B1	A0B2
	Sharing banner (A1)	A1B0	A1B1	A1B2

Outcomes and hypotheses

Primary outcome 1 (sharing): Sharing the email on social media or forwarding to others. This is a binary variable in which clicking on the pay it forward link, or clicking on any of the social media sharing or forwarding icons has been treated as one. We expected the sharing banner would increase sharing and forwarding (H1).

Primary outcome 2 (interaction): Interacting with the email by clicking on links contained in it. This is a binary variable in which clicking on any hyperlinks in the email with the exception of any social media forwarding or sharing icons is treated as one. We expected the 'heuristic icons' would—jointly and separately—increase interaction with the emails (H2, H3 and H4).

Primary outcome 3 (email open rates): opening the email. This is a binary variable, in which a value of one indicates that the email was definitely opened. As discussed further below, we updated the PAP to include this outcome variable and the following hypothesis: we expected the 'heuristic icons' would increase open rates as it may be possible for them to be seen in preview mode without actually opening the email (H5).

Secondary outcome (type of interaction): Printing or saving the email to refer to later (more intensive interaction). This is a binary variable, focusing only on a subset of primary outcome 2, treated as one if print or save links were clicked. As noted below, we updated the PAP to include this outcome variable and the following hypothesis. We expected the 'heuristic icons' would increase clicks to print or save (H2 extension and H3 extension).

Missing values in all of these outcomes (that is, where the email was sent and bounced) were coded as zero.

Changes to initial pre-analysis plan (PAP) and deviations from updated PAP

The analysis in this report involved one deviation from the *updated* pre-analysis plan that was lodged on 8 April 2020. This related to an unanticipated loss of sample between randomisation and mail out (described in more detail below under 'Study population, sample size and randomisation'). After we had completed the split into test and holdout data sets, and completed our analysis, we discovered that 6,196 subscribers (or ex-subscribers) had been excluded from the final data set and not been sent an email. As a robustness check, we repeated our analysis after adding those observations back in and setting their outcomes to zero. As expected, there were only minimal differences in the results.

Updates to the *initial* PAP, based on analysis of the test data set, were described in the updated PAP and are summarised as follows.

Email open rates: Contrary to our expectations in the initial PAP, we observed material differences in email open rates between emails with icons and those without. We speculated that, before actually opening the email, some people may see the email in preview mode and those who saw the icons were more inclined to open the email. This led to two changes in the updated PAP.

- First, the original hypotheses H1-H4 were tested on the full data set, not just the subset of the data with those who opened the email (that is, we reverted to conducting a pure intent-to-treat (ITT) analysis).
- Second, we added a new binary outcome variable for email open rates and a new hypothesis (H5) that emails containing icons would show significantly higher open rates than those that contain no icons.

Factorial design and interaction effects: In the original PAP, we pre-specified that we would conduct tests using both a short-form model (without interactions) and a long-form model (including interactions). The results from the test data showed material differences in both effect sizes and p-values between the two models. Consequently, we followed the recommendation of Muralidharan, Romero and Wuthrich (2020) and used the long-form

model with interactions for our main analysis for all hypotheses. However, we have also reported the short-form model in the statistical tables that follow, so differences between the two models can be observed.

Type of interaction with email: We hypothesised that the timing icon would increase interaction with emails (H2). Exploratory analysis of the test data suggested that increased interaction with emails due to the 'timing icon' mainly related to a particular type of interaction—clicking on the 'print and save' link. We added a hypothesis, contingent on replication of H2, that the timing icon increased interaction with 'print and save' more than on other embedded links.

Study population, sample size and randomisation

The sample frame for this trial was the entire subscriber base for the Stay Smart Online email Alert Service at the time of implementation (that is, around a week prior to sending the emails, to allow for randomisation): 60,508 individuals. Subscribers who signed-up to the service after the date of randomisation were not included in the trial. They were sent the same email as those in the control condition, but their results were excluded from the analysis.

Subscribers were randomised (using a STATA script) into one of six groups, with a balanced allocation ratio, using complete randomisation. Another BETA staff member not directly involved in the project verified the randomisation code. After randomisation, the six email lists were uploaded to the mailing platform. The email addresses were automatically matched against a master list of people who had previously unsubscribed or recorded a hard bounce (that is, if the email address no longer exists), and no email alert was sent to these addresses. This reduced the size of the final sample who were sent the emails to 54,312. This sample was used for the analysis, and any emails that were sent, but bounced after that, were retained in the data, and were treated as having values of zero for all outcome variables.

To split the data into test and holdout datasets, a BETA analyst used the block_ra command (from the Randomizer package in R) to stratify by treatment status to ensure balanced assignment across the two datasets and then saved them separately. Another analyst performed the analysis in STATA on the test dataset. Following adjustments to the pre-analysis plan, the analysis was repeated on the holdout dataset. Results from both can be seen in Key statistical tables.

Power calculations

Our original power analysis suggested that, with an alpha (significance level) of 0.01, we had 95% power in both the test and holdout samples to detect:

- An increase in interaction (clicks) from 8% to 9.8%
- An increased in sharing from 2% to 3%.

We did not update the power analysis after we updated the pre-analysis plan.

Method of analysis

We used ordinary least squares (OLS) regression to estimate our main effects. These estimates, confidence intervals and p-values were derived from a model with the following specification:

$$y = \alpha + \tau_1 A + \tau_2 B + \tau_3 C + \tau_4 AB + \tau_5 AC + \epsilon$$

where y is our outcome, α is the intercept, $\tau_1$is the main effect of including a Sharing banner, τ_2 is the main effect of including the first set of icons, τ_3 is the main effect of including the second set of icons, τ_4 and τ_5 are interaction terms for A×B and A×C, respectively, and ε is an error term which picks up variance not explainable by treatment indicators.

As noted above, we specified this long-form model (with the interaction terms) as our primary analysis in the updated pre-analysis plan (PAP). The original PAP specified both short-form and long-form models. We also report the short-form results in the statistical tables below as a robustness check.

Missing values

Some individuals who were randomised into the trial and who were subsequently sent the email did not receive it (if the email bounced, for example). These individuals were still included in the analysis and their outcomes were coded as not having interacted or shared.

Randomisation was applied to the full subscriber list. As noted above, it was only after randomisation that this list was compared against a list of emails that had previously unsubscribed or hard bounced (soft bounce includes things like a mailbox being full or message exceeding a size limit). These email addresses were never sent an email, and were subsequently excluded from the analysis, even though they were originally randomised. This was a departure from intent-to-treat analysis however those subscribers' missingness must be independent of their potential outcomes (MIPO) because they were missing before the intervention was delivered. Furthermore, we conducted a robustness check by adding a random sample of half the missing subscribers to the holdout data and then repeating the analysis. There was no material change in our results.

Key statistical tables

Overview

This appendix presents the statistical analyses and robustness checks undertaken for the email alert service study. It is divided into two parts.

First, we present details of the random assignment to treatment cells, and randomisation to test and holdout data sets (Table 2 and Table 3). This includes the missing data described in Missing values.

Second, we present the results of the primary analysis using the holdout data and long-form model (that is, allowing for interactions in the factorial design). For each set of results, we also present the results from the test data and from the short-form model. Specifically, the tables present the effect of:

- a sharing banner on forwarding and sharing (Table 4 and Table 5)
- an action or timing icon, compared to control, on interaction with the email (Table 6 and Table 7)
- an action versus a timing icon, on interaction with the email (Table 8 and Table 9)
- any icon, compared to control, on email open rates (Table 10 and Table 11)
- an action or timing icon, compared to control, on email open rates (Table 12 and Table 13)
- an action or timing icon, compared to control, on printing or saving the email (Table 14 and Table 15).

Randomisation and missing data

As detailed in Missing values, some observations were excluded after randomisation but before mailout, and these were excluded from the subsequent analysis. Those ‘unsent’ emails comprised (on average) 10.2 per cent of the original subscriber list, or 6,196 subscribers (Table 2). As a robustness check, half of the ‘unsent’ subscribers were added back into the holdout data set and coded as zero on all outcomes and the same analysis code was run over the data set. This made no difference other than to make most p-values slightly higher, but not materially so.

Table 3 lays out the relationship between treatment cells, the factorial design, and the sample sizes associated with each group for the holdout data. The holdout data is the basis for our main analysis and results cited in the report, but results from the test data are also provided in the regression output tables below.

Table 2. Number of subscribers randomised to each treatment cell.

Treatment cell	Number randomised to cell	Unsent	Unsent (%)	Test data set	Holdout data set
A0B0	10,084	979	9.7%	4,553	4,552
A0B1	10,085	1,032	10.2%	4,527	4,526
A0B2	10,085	1,018	10.1%	4,534	4,533
A1B0	10,085	1,105	11.0%	4,490	4,490
A1B1	10,084	1,002	9.9%	4,541	4,541
A1B2	10,085	1,060	10.5%	4,513	4,512
Total	**60,508**	**6,196**	**10.2%**	**27,158**	**27,154**

Table 3. Number of subscribers in each treatment group, holdout data only

	Standard (B0)	Timing icon (B1)	Action icon (B2)
No sharing banner (A0)	4,552	4,526	4,533
Sharing banner (A1)	4,490	4,541	4,512

Results

We present the linear regression output for the hypotheses listed in Technical in Table 4 to Table 15. The results for a long-form model using the holdout data are presented first and in bold, as these are the main results as specified in the pre-analysis plan. As a robustness check, we also present the results from the test data and results from a short-form model. We also conducted logistic regressions as a further robustness check but results did not differ materially from the OLS results, so are not included here.

One-sided hypotheses are presented with a single-sided confidence interval. The group sample size is n. Means, treatment effects, 95 per cent confidence intervals and p-values are derived from adjusted linear regression models (see Method of analysis). Occasionally, the difference in the reported means is slightly different from the effect estimates: this is due to rounding error.

Table 4. H1 - Impact of 'sharing banner' on forwarding/sharing the email (long-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	**Control**	**13,611**	**0.29%**				
Holdout data	**Sharing**	**13,543**	**0.85%**	**0.00561**	**0.00301**	**N.A.**	**<0.001**
Test data	Control	13,614	0.22%				
Test data	Sharing	13,544	0.71%	0.00493	0.00257	N.A.	<0.001

Table 5. H1 - Impact of 'sharing banner' on forwarding/sharing the email (short-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	Control	13,611	0.30%				
Holdout data	Sharing	13,543	0.78%	0.00474	0.00328	N.A.	<0.001
Test data	Control	13,614	0.26%				
Test data	Sharing	13,544	0.69%	0.00429	0.00293	N.A.	<0.001

Table 6. H2 and H3 - Impact of timing and action icons on interaction with email (long-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	**No icon**	**9,042**	**2.94%**				
Holdout data	**Timing**	**9,067**	**3.56%**	**0.00613**	**0.00001**	**N.A.**	**0.050**
Holdout data	**Action**	**9,045**	**3.26%**	**0.00321**	**-0.00278**	**N.A.**	**0.189**
Test data	No icon	9,043	2.53%				
Test data	Timing	9,068	3.40%	0.00876	0.00291	N.A.	0.007
Test data	Action	9,047	2.96%	0.00430	-0.00134	N.A.	0.105

Table 7. H2 and H3 - Impact of timing and action icons on interaction with email (short-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	No icon	9,042	2.94%				
Holdout data	Timing	9,067	3.53%	0.00588	0.00155	N.A.	0.013
Holdout data	Action	9,045	3.36%	0.00419	-0.00008	N.A.	0.054
Test data	No icon	9,043	2.68%				
Test data	Timing	9,068	3.12%	0.00445	0.00035	N.A.	0.037
Test data	Action	9,047	2.88%	0.00209	-0.00194	N.A.	0.197

Table 8. H4 - Action vs timing icons, impact on interaction with email (long-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (two-sided)
Holdout data	**Action**	**9,045**	**3.26%**				
Holdout data	**Timing**	**9,067**	**3.56%**	**0.00292**	**-0.00455**	**0.01040**	**0.444**
Test data	Action	9,047	2.96%				
Test data	Timing	9,068	3.40%	0.00446	-0.00276	0.01170	0.226

Table 9. H4 - Action vs timing icons, impact on interaction with email (short-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (two-sided)
Holdout data	Action	9,045	3.36%				
Holdout data	Timing	9,067	3.53%	0.00168	-0.00363	0.00699	0.535
Test data	Action	9,047	2.88%				
Test data	Timing	9,068	3.12%	0.00237	-0.00261	0.00734	0.351

Table 10. H5 - Impact of any icon on email open rates (long-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	**No icon**	**9,042**	**42.97%**				
Holdout data	**Any icon**	**18,112**	**44.24%**	**0.01270**	**-0.00208**	**N.A.**	**0.079**
Test data	No icon	9,043	42.32%				
Test data	Any icon	18,115	44.10%	0.01780	0.00298	N.A.	0.024

Table 11. H5 - Impact of any icon on email open rates (short-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	No icon	9,042	42.47%				
Holdout data	Any icon	18,112	43.69%	0.01220	0.00176	N.A.	0.027
Test data	No icon	9,043	41.70%				
Test data	Any icon	18,115	43.94%	0.02240	0.01200	N.A.	<0.001

Table 12. H5 extension - Impact of timing and action icons on email open rates (long-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	**No icon**	**9,042**	**42.97%**				
Holdout data	**Timing**	**9,067**	**43.88%**	**0.00910**	**-0.00802**	**N.A.**	**0.191**
Holdout data	**Action**	**9,045**	**44.61%**	**0.01640**	**-0.00076**	**N.A.**	**0.058**
Test data	No icon	9,043	42.32%				
Test data	Timing	9,068	43.94%	0.01610	-0.00097	N.A.	0.061
Test data	Action	9,047	44.27%	0.01940	0.00232	N.A.	0.031

Table 13. H5 extension - Impact of timing and action icons on email open rates (short-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	No icon	9,042	42.47%				
Holdout data	Timing	9,067	43.40%	0.00935	-0.00275	N.A.	0.102
Holdout data	Action	9,045	43.98%	0.01510	0.00302	N.A.	0.020
Test data	No icon	9,043	41.70%				
Test data	Timing	9,068	43.75%	0.02050	0.00840	N.A.	0.003
Test data	Action	9,047	44.14%	0.02440	0.01230	N.A.	<0.001

Table 14. H2 and H3 extension - Impact of timing and action icons on printing and saving (long-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	**No icon**	**9,042**	**0.94%**				
Holdout data	**Timing**	**9,067**	**1.59%**	**0.00646**	**0.00260**	**N.A.**	**0.003**
Holdout data	**Action**	**9,045**	**1.52%**	**0.00578**	**0.00197**	**N.A.**	**0.006**
Test data	No icon	9,043	0.79%				
Test data	Timing	9,068	1.50%	0.00711	0.00344	N.A.	<0.001
Test data	Action	9,047	1.24%	0.00444	0.00099	N.A.	0.017

Table 15. H2 and H3 extension - Impact of timing and action icons on printing and saving (short-form model)

Data	Treatment Group	*n*	Mean	Effect	95% Confidence Interval		p-value (one-sided)
Holdout data	No icon	9,042	0.95%				
Holdout data	Timing	9,067	1.47%	0.00516	0.00249	N.A.	<0.001
Holdout data	Action	9,045	1.48%	0.00530	0.00262	N.A.	<0.001
Test data	No icon	9,043	0.83%				
Test data	Timing	9,068	1.37%	0.00538	0.00284	N.A.	<0.001
Test data	Action	9,047	1.22%	0.00386	0.00140	N.A.	0.005

Cyber security survey for small and medium business

Technical details

Overview of the Small and Medium Business (SMB) survey experiment

We conducted an individually randomised survey experiment delivered as part of a survey collecting information on the cybersecurity behaviours of small and medium businesses (SMBs). The survey and experiment were collected through an online survey platform (Qualtrics).

The initial survey and subsequent experiment were structured as follows. First, respondents completed the initial survey, which took roughly nine minutes to complete on average. Then, respondents were randomly allocated into one of four groups and exposed to the different versions of the intervention (information about detecting phishing emails, software updates and backing up data). Next, individuals completed a second short survey (the 'outcome survey') to gather outcome data. Finally, all respondents were invited to participate in a follow-up survey, which was identical for all treatment groups.

The initial experimental design was piloted on a sample of 461 individuals, and we used this pilot to refine our interventions.

The final survey was distributed via a small business e-newsletter to approximately 2.4 million businesses, who were able to opt in to complete the survey (without incentive). Of these, 1,553 individuals (0.06 per cent) commenced the survey and 1,186 individuals completed the main body of the survey and were subsequently randomised into the experiment.

Pre-registration and pre-analysis plans

The trial was listed on the BETA website project page on 6 November 2019. We pre-registered on the American Economic Association RCT Registry (RCT ID no. AEARCTR-0004957) under the title 'Engaging small business in cyber safe practice' on 29 October 2019. An updated pre-analysis plan was uploaded on 30 October 2019, before analysis had commenced but after completion of the trial. A further edit to the names of the primary investigators was made to the pre-registration on 19 November. There were no deviations from our pre-analysis plan.

Interventions

Individuals were randomised into four groups: the control group and three treatment groups. The control group proceeded directly to the outcome survey without exposure to any information or advice. The treatment groups received one of the following three interventions:

T1. Plain text—Respondents received information/advice about detecting phishing emails, software updates and backing up data (Figure 3).

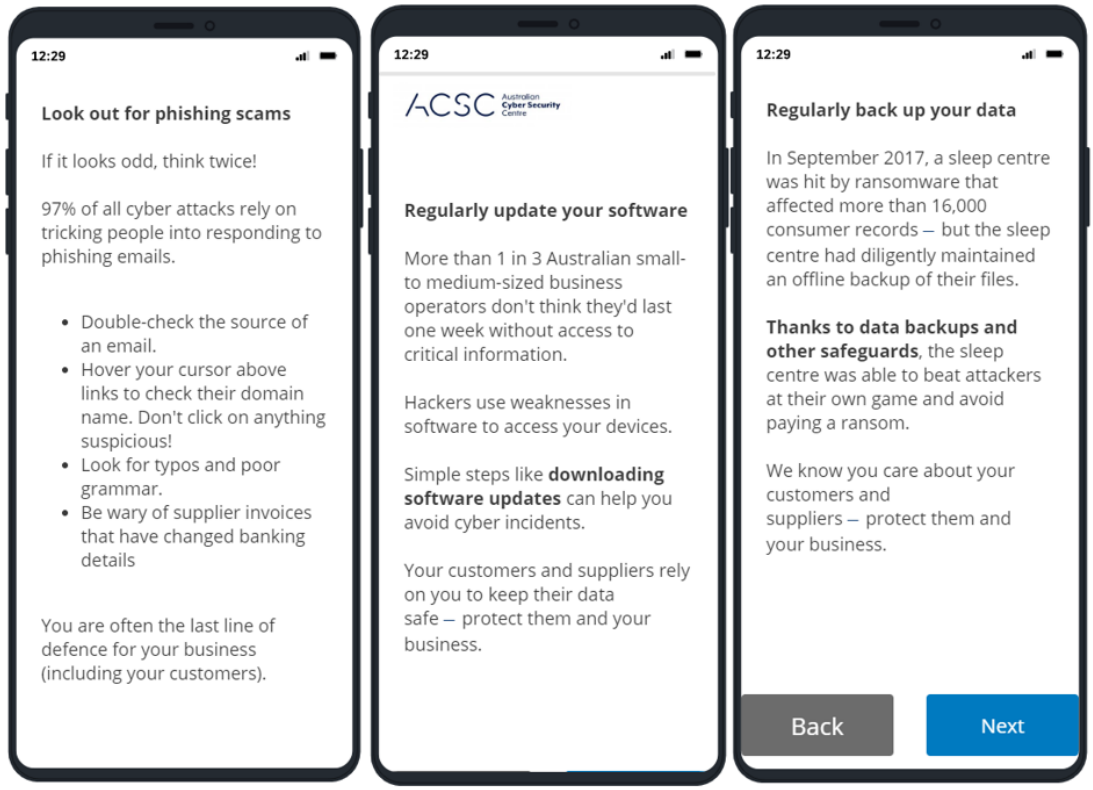


Figure 3: Plain text interventions

T2. Infographic—Respondents received the same information/advice as above, but presented as an infographic (Figure 4).

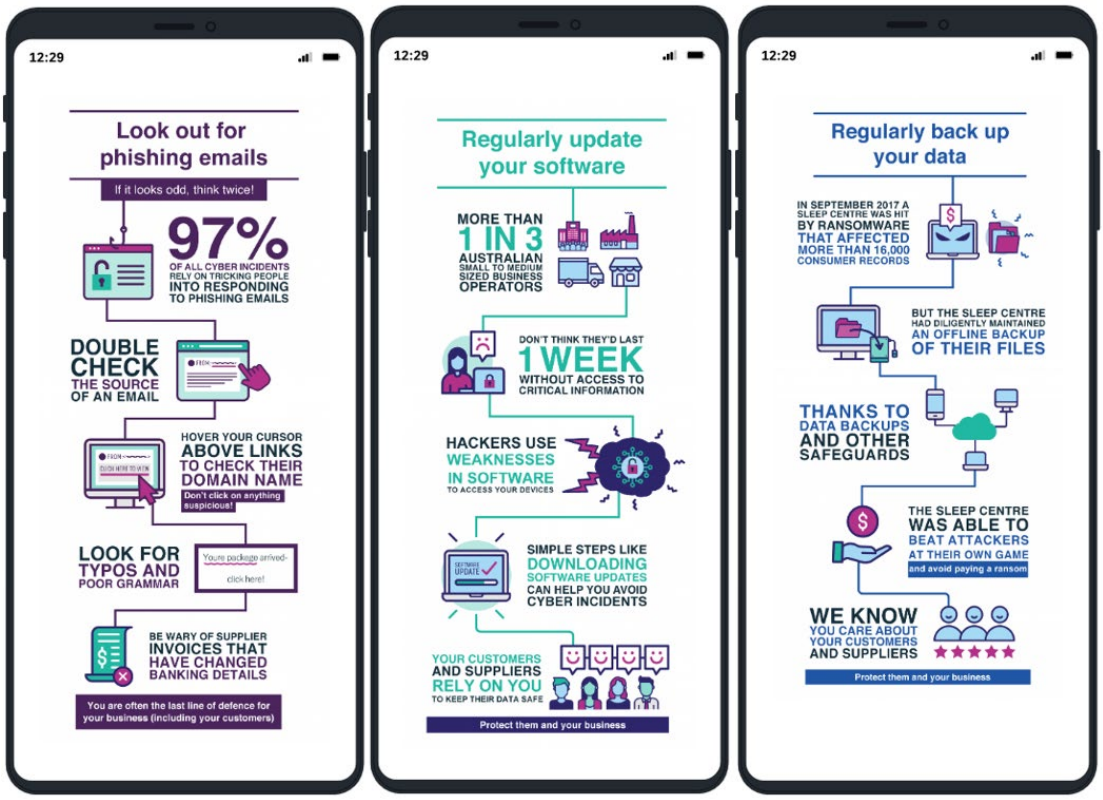


Figure 4: Infographic interventions

T3. Interactive infographic—Respondents received a quiz-style question on each topic, followed by the previous infographic explaining the correct answer (Figure 5).

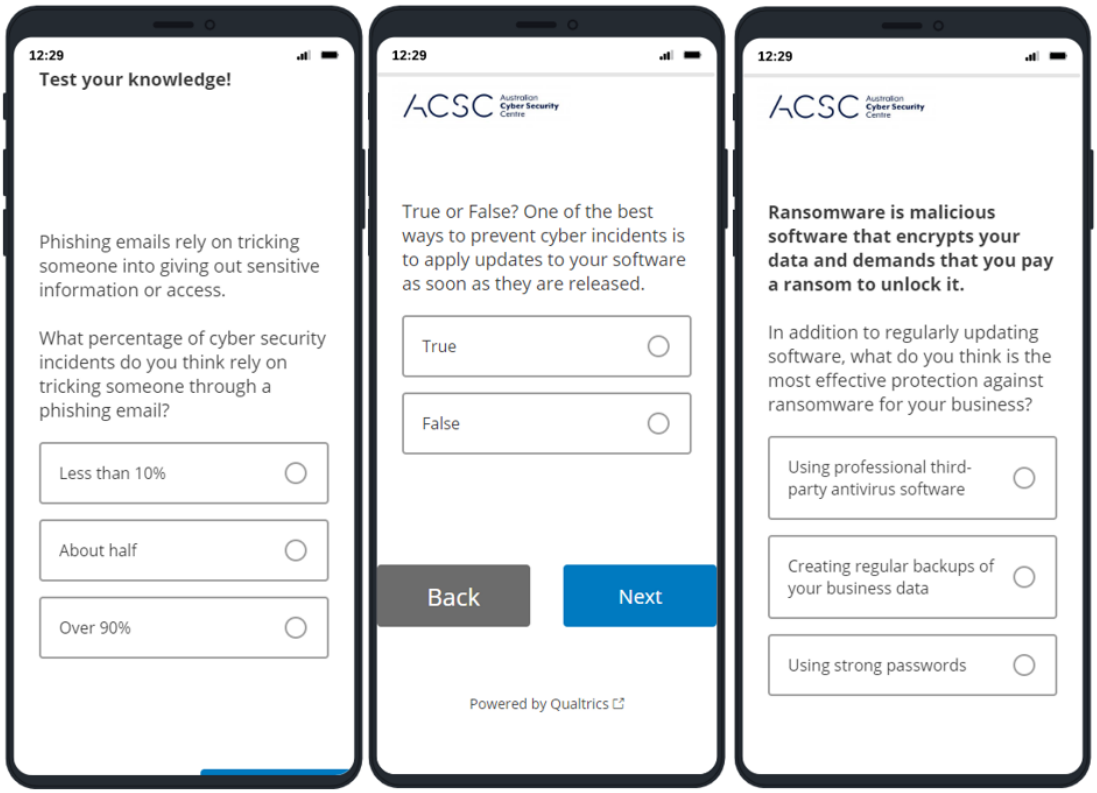


Figure 5: Interactive interventions

Outcomes and hypotheses

The study had three primary outcomes.

Primary Outcome 1 (phishing test score)—Individuals completed a phishing test where they were presented with three emails (one genuine, two fake) and asked to decide if they were genuine or fake (). The outcome was measured as the average number of correct answers. We expected those who received any of the interventions would score higher on the phishing test than those in the control group (H1).

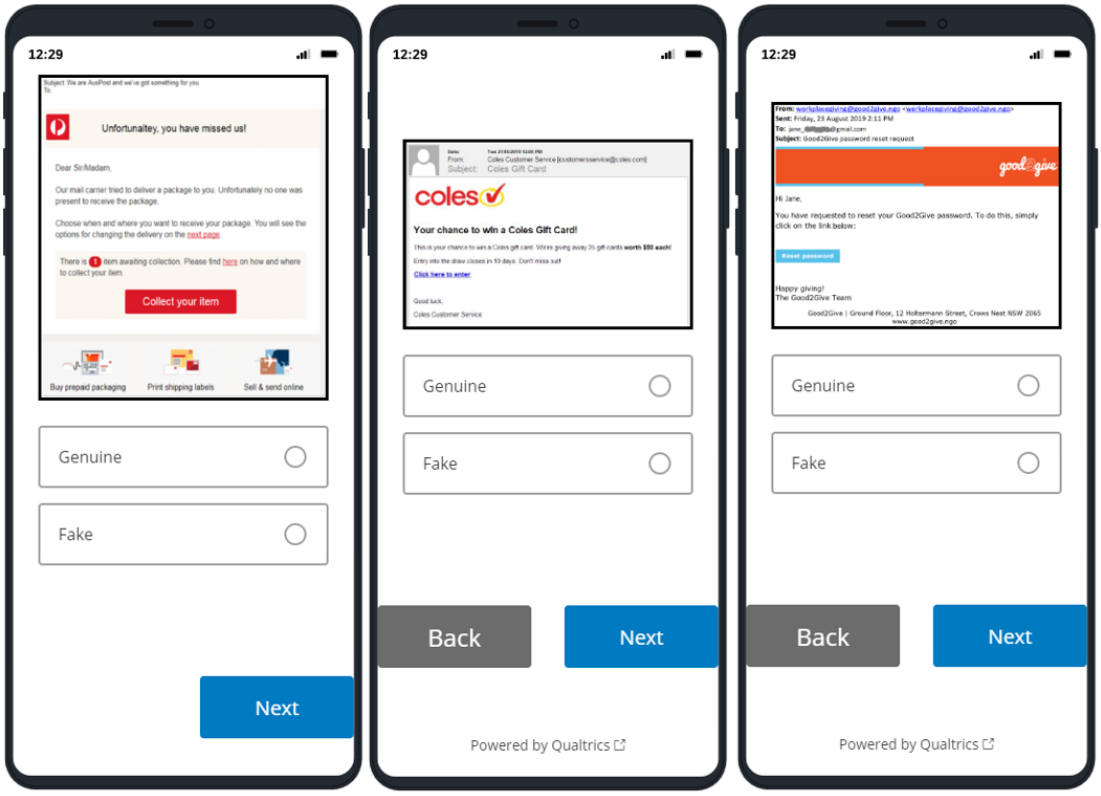


Figure 6: Phishing test

Primary Outcomes 2 and 3 (self-reported outcomes)—We asked individuals about their intentions to update their software and back up their data. The questions presented were as follows:

1. Thinking about the next seven days, how likely are you to check for software updates, as required, on your business devices?
2. Thinking about the next seven days, how likely are you to initiate regular backups of business data?'

For both of these outcomes, response options were identical: System is already in place, Definitely, Likely, Unlikely, Definitely not. The outcome was derived as a binary variable in which responses of 'System is already in place' and 'Definitely' equalled one and 'Likely', 'Unlikely, and 'Definitely not' equalled zero. We expected that individuals who received any of the interventions would be more likely to say they intended to check for software updates and initiate regular backups of business data (H2 and H3).

For these outcomes we also performed a secondary analysis in which we treat the survey scale as continuous (but collapsing 'System already in place' and 'Definitely' together).

Secondary Outcome 1—RCT participants were asked to participate in a follow-up survey three weeks later. In this survey, we asked a number of questions relating to phishing, update and backup behaviours, with between 227 and 229 responding to the relevant follow-up outcome questions.

The follow-up phishing outcome was measured with a set of three questions from the Human Aspects of Information Security Questionnaire (HAIS-Q; Hadlington, Parsons, Calic and Butavicius 2019). The three questions were on a five-point scale from Strongly disagree to Strongly agree, and were as follows:

1. If an email comes from someone I know, I don't always click on the link.
2. If an email from an unknown sender looks interesting, I click on the link.
3. I don't open email attachments if I don't know the sender.

These were summed to create a total score from 0-12, in which a high score is equivalent to safer email behaviours (the second question was reverse coded).

The follow-up questions on software updates and data backups were as follows:

1. Does you business install software updates?
2. Does you business back up information on all devices (or store in the cloud)?

Responses were on a seven-point scale: Yes, automatically; Yes, frequently; Yes, usually; Sometimes; Not usually; Not at all; Not to my knowledge. Values of *Yes, automatically* or *Yes, frequently* were treated as one, otherwise zero.

Study population, sample size and randomisation

The study population was small and medium businesses, and an invitation to participate was sent to all small and medium businesses in Australia through the ATO small business newsroom mailing list. There was no incentive to participate and we had a final sample of 1,186, which gave us between 280 and 292 individuals per group. Randomisation occurred through the Qualtrics platform using complete randomisation at the point where an individual had completed the survey component and was progressing to the experiment component.

Power calculations

Our power calculations assumed we would have 250 individuals in each group. We used the baseline prevalence levels for our outcomes from our pilot RCT. Based on these calculations our trial had the power to calculate the following effect sizes at 80% power and a 5% significance level:

- A minimum effect size of 0.25 (cohen's h) on the phishing test
- A minimum effect of 10.5 percentage points on the software updates intention question
- A minimum effect of 8.6 percentage points on the data backups intention question

Method of analysis

We used an Ordinary Least Squares (OLS) model for our primary analysis with the following specification:

$$y_i = \alpha + \tau T_i + \beta x_i + \gamma x_i T_i + \varepsilon_i$$

where y is an outcome variable, α is the intercept, T_i is a vector of indicators for treatment group membership, x_i is a vector of mean-centred covariates (see Covariates below), $x_i T_i$ is an interaction between treatment group indicators and the mean-centred covariates, and ε is an error term which picks up variance not explained by treatment indicators or covariates.

Covariates

For each hypothesis, we included six covariates (Table 16). These were derived from questions in the baseline survey prior to randomisation, and selected based on a series of regressions on the pilot dataset.

Table 16. List of covariates

Covariate description	Derived from	Type	Included for outcome
Past email behaviours	HAIS Q email behaviours score (0/12) split above and below median	Binary	Outcome 1 only (phishing test)
Past behaviour: downloading software updates	Self-rated “automatically or frequently updates software”	Binary	Outcome 2 only (software updates)
Past behaviour: backing up data	Self-rated “automatically or frequently backs up data”	Binary	Outcome 3 only (data backup)
Business gross income	>=$250,000	Binary	All
Cyber security knowledge	Self-rated “above average knowledge”	Binary	All
Cyber security importance	Self-rated “cyber security of high importance”	Binary	All
Cyber security annual spend	>=$500	Binary	All
Device type	Desktop versus mobile device (from Qualtrics metadata)	Binary	All

We included device type (recorded by Qualtrics) because the interventions and phishing test looked slightly different on a mobile device compared to a larger screen. Also, when the phishing test was viewed on a mobile device, it was not possible to ‘hover’ the cursor over URLs, so the URLs were inserted statically.

Multiple comparison adjustments

In our pre-analysis plan, we stated that we would not make adjustments for multiple comparisons for our primary analysis however we committed to supplement our results with Bonferroni-adjusted p-values. This section describes how we implemented this adjustment, and also sets out some cautionary notes about interpreting the adjusted p-values.

When we make multiple comparisons in relation to the same theoretical claim, we inflate our family-wise error rate (FWER) above our threshold for statistical significance five per cent. That is, for studies where the null hypothesis is true, we increase the probability we will find a false positive.

We only need to adjust for comparisons within the same 'family' of claims (see, for example, Lakens 2016). We see our study as testing two theories or families. First, providing information about cyber risks (rather than not) will improve understanding of these risks and how to address them, and hence it will increase knowledge or intentions to take steps to reduce those risks. We tested each of these for three different risks (phishing, software updates, and data backups). We also tested three variations of how the information was presented (plain text, infographic, or interactive infographic). This gives a total of nine tests or comparisons within this family.[1]

Our second theory was that variations in the presentation of information will have different effects on understanding and intentions. Again, we tested this for three different risks and, because we had three presentations, we had another three variations (that is, T1 versus T2, T1 versus T3 and T2 versus T3). Thus, we had another nine tests for our second family.

We chose to use a Bonferroni adjustment even though it is unduly conservative because it is simple and well known, and we are unaware of a simple, suitable alternative for our study. Bonferroni is unduly conservative because it assumes each of the comparisons are independent from one another when, in our study, most of our comparisons were correlated (for example, because they involved the same treatment group several times). Consequently, the Bonferroni-adjustment will reduce the family-wise error rate well below five per cent and produce a corresponding *increase* in the false-negative error rate. For this reason, we did not use Bonferroni-adjusted p-values for our primary analysis.

Missing data

We expected there to be missing outcome data due to people leaving the survey prior to completing the outcome measures, as well as due to skipping individual questions (there were no forced responses). We considered this unlikely to be related to treatment status, and found no evidence of differential attrition.

Survey respondents who were randomised but did not provide a response for a given outcome were excluded from the analysis for that outcome (but included for other outcomes if they provided a response).

[1] We also conducted a pooled test of the three 'information groups' against control but we did not count this as an extra test since it was more akin to a preliminary joint test of significance before proceeding with separate tests for each arm against control.

We included missingness dummies to account for missing covariate data.

Generalisability of results

Non-response bias is likely to have been an issue as the kinds of businesses who respond to an online survey about cyber security may be different in many ways to those who do not. This creates an issue around generalisability. First, it is difficult to say whether the individuals who respond to an online survey about cyber security will be similar to or different from those who might visit the Australian Cyber Security Centre Website in search of advice about an aspect of cyber security. Second, the degree to which an expressed intention to perform an action correlates with actual implementation likely varies. Together, these things mean that while our results make us confident that the intervention heightened intentions (and awareness), we feel unable to accurately assess how many businesses stand to implement changes to their cyber security behaviours if this intervention were rolled out systematically on the ACSC website. However, the cost of these interventions is low and the risks seem also low as changes were in the expected direction.

Key statistical tables

Overview

This appendix presents the statistical analyses and robustness checks undertaken for the small and medium businesses survey experiment. We present the results of the primary analysis using a binary outcome variable and a continuous outcome variable for each model. For each hypothesis, results are presented for the three primary outcomes: performance in the phishing test, intention to update software, and intention to back up data. Specifically, the tables present the effect of:

- H1: Pooled treatments versus control (Table 17 to Table 19)
- H2: Each treatment versus control. In addition to primary outcomes, tables include the follow-up survey results, three weeks later, for: HAIS Q email behaviours scale, software behaviours, and back up behaviours (Table 20 to Table 22).
- H3: Infographic versus plain text (Table 23 to Table 25)
- H4: Interactive versus plain text (Table 26 to Table 28)
- H5: Interactive versus infographic condition (Table 29 to Table 31)

Results

We present the linear regression output for the hypotheses listed in the previous chapter in Table 17 to Table 31. The results for a primary hypothesis are presented first and in bold, as these are the main results as specified in the pre-analysis plan. As a robustness check, we also present the results for the phishing test as a binary variable (1 = Scored all correct on phishing test), and the results for the software updates and data backup intentions questions in which intention is coded as a continuous variable (Likert score 0-3).

One-sided hypotheses are presented with a single-sided confidence interval. The group sample size is n. Means, treatment effects, 95 per cent confidence intervals and p-values are derived from adjusted linear regression models (see Method of analysis in the previous chapter. Occasionally the difference in the reported means is slightly different from the effect estimates: this is due to rounding error.

Table 17. H1 - Pooled treatments versus control: phishing test score

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)
Score on phishing test (continuous)						
Control (reference)	**291**	**0.70**				
Pooled treatments	**849**	**0.72**	**0.020**	**-0.005**	**N.A.**	**0.098**
Scored all correct on phishing test (binary)						
Control (reference)	291	27%				
Pooled treatments	849	30%	0.029	-0.021	N.A.	0.170

Table 18. H1 - Pooled treatments versus control: intention to update software

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)
Strong intention to update software (binary)						
Control (reference)	**292**	**79%**				
Pooled treatments	**848**	**87%**	**0.083**	**0.044**	**N.A.**	**<0.001**
Likert score on intention to update software (continuous, 0-3 scale)						
Control (reference)	292	2.71				
Pooled treatments	848	2.82	0.108	0.048	N.A.	0.002

Table 19. H1 - Pooled treatments versus control: intention to back up data

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)
Strong intention to back up data (binary)						
Control (reference)	**292**	**82%**				
Pooled treatments	**850**	**88%**	**0.063**	**0.029**	**N.A.**	0.001
Likert score on intention to back up data (continuous, 0-3 scale)						
Control (reference)	292	2.79				
Pooled treatments	850	2.84	0.050	0.008	N.A.	0.025

Table 20. H2 - Each treatment versus control: phishing test score

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Score on phishing test (continuous)							
Control (reference)	**291**	**0.70**					
Text	**283**	**0.71**	**0.018**	**-0.013**	**N.A.**	**0.174**	**1.0**
Infographic	**282**	**0.69**	**-0.002**	**-0.034**	**N.A.**	**0.545**	**1.0**
Interactive	**284**	**0.74**	**0.045**	**0.015**	**N.A.**	**0.007**	**0.061**
Scored all correct on phishing test (binary)							
Control (reference)	291	27%					
Text	283	29%	0.018	-0.043	N.A.	0.314	N.A.
Infographic	282	27%	0.002	-0.058	N.A.	0.474	N.A.
Interactive	284	34%	0.072	0.010	N.A.	0.028	N.A.
Score on HAIS Q measure - three weeks later (continuous)							
Control (reference)	51	0.83					
Text	63	0.84	0.007	-0.035	N.A.	0.391	N.A.
Infographic	50	0.80	-0.034	-0.084	N.A.	0.866	N.A.
Interactive	63	0.81	-0.026	-0.070	N.A.	0.831	N.A.

Table 21. H2 - Each treatment versus control: intention to update software

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Strong intention to update software (binary)							
Control (reference)	**292**	**79%**					
Text	**283**	**89%**	**0.104**	**0.059**	**N.A.**	**<0.001**	**<0.001**
Infographic	**280**	**88%**	**0.098**	**0.054**	**N.A.**	**<0.001**	**0.001**
Interactive	**285**	**83%**	**0.045**	**-0.004**	**N.A.**	**0.065**	**0.581**
Likert score on intention to update software (continuous, 0-3 scale)							
Control (reference)	292	2.71					
Text	283	2.86	0.151	0.083	N.A.	<0.001	N.A
Infographic	280	2.84	0.130	0.061	N.A.	0.001	N.A
Interactive	285	2.75	0.041	-0.036	N.A.	0.191	N.A
Updated software - three weeks later (binary)							
Control (reference)	51	91%					
Text	63	95%	0.041	-0.039	N.A.	0.200	N.A
Infographic	52	93%	0.024	-0.066	N.A.	0.333	N.A
Interactive	63	93%	0.028	-0.050	N.A.	0.275	N.A

Table 22. H2 - Each treatment versus control: intention to back up data

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Strong intention to back up data (binary)							
Control (reference)	**292**	**82%**					
Text	**283**	**88%**	**0.063**	**0.022**	**N.A.**	**0.006**	**0.050**
Infographic	**281**	**88%**	**0.062**	**0.021**	**N.A.**	**0.006**	**0.054**
Interactive	**286**	**88%**	**0.059**	**0.019**	**N.A.**	**0.008**	**0.069**
Likert score on intention to back up data (continuous, 0-3 scale)							
Control (reference)	292	2.79					
Text	283	2.86	0.064	0.013	N.A.	0.019	N.A
Infographic	281	2.85	0.052	0.000	N.A.	0.049	N.A
Interactive	286	2.83	0.035	-0.020	N.A.	0.149	N.A
Implemented backups - three weeks later (binary)							
Control (reference)	51	82%					
Text	62	84%	0.019	-0.092	N.A.	0.387	N.A
Infographic	52	80%	-0.014	-0.120	N.A.	0.417	N.A
Interactive	63	78%	-0.040	-0.153	N.A.	0.281	N.A

Table 23. H3 - Infographic versus plain text: phishing test score

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Score on phishing test (continuous)							
Text (reference)	**283**	**0.71**					
Infographic	**282**	**0.70**	**-0.018**	**-0.055**	**0.019**	**0.337**	**1.0**
Scored all correct on phishing test (binary)							
Text (reference)	283	29%					
Infographic	282	27%	-0.013	-0.088	0.062	0.733	N.A.

Table 24. H3 - Infographic versus plain text: intention to update software

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Strong intention to update software (binary)							
Text (reference)	**283**	**89%**					
Infographic	**280**	**88%**	**-0.005**	**-0.054**	**0.043**	**0.832**	**1.0**
Likert score on intention to update software (continuous, 0-3 scale)							
Text (reference)	283	2.86					
Infographic	280	2.84	-0.021	-0.093	0.051	0.566	N.A.

Table 25. H3 - Infographic versus plain text: intention to back up data

H3 Backups							
Treatment group	***n***	**Mean**	**Effect (relative to reference)**	**95% Confidence Interval**		**p-value (one-sided)**	**p-value (bonferroni corrected)**
Strong intention to back up data (binary)							
Text (reference)	**283**	**88%**					
Infographic	**281**	**88%**	**0.000**	**-0.046**	**0.046**	**0.997**	**1.0**
Likert score on intention to back up data (continuous, 0-3 scale)							
Text (reference)	283	2.85					
Infographic	281	2.84	-0.011	-0.073	0.051	0.724	N.A.

Table 26. H4 - Interactive versus plain text: phishing test score

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Score on phishing test (continuous)							
Text (reference)	**283**	**0.72**					
Interactive	**284**	**0.74**	**0.024**	**-0.011**	**0.060**	**0.175**	**1.0**
Scored all correct on phishing test (binary)							
Text (reference)	283	29%					
Interactive	284	34%	0.051	-0.025	0.128	0.186	N.A.

Table 27. H4 - Interactive versus plain text: intention to update software

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Strong intention to update software (binary)							
Text (reference)	**283**	**89%**					
Interactive	**285**	**83%**	**-0.056**	**-0.109**	**-0.004**	**0.037**	**0.330**
Likert score on intention to update software (continuous, 0-3 scale)							
Text (reference)	283	2.86					
Interactive	285	2.75	-0.105	-0.187	-0.024	0.012	N.A.

Table 28. H4 - Interactive versus plain text: intention to back up data

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Strong intention to back up data (binary)							
Text (reference)	**283**	**88%**					
Interactive	**286**	**88%**	**-0.001**	**-0.048**	**0.047**	**0.983**	**1.0**
Likert score on intention to back up data (continuous, 0-3 scale)							
Text (reference)	283	2.85					
Interactive	286	2.83	-0.027	-0.094	0.039	0.419	N.A.

Table 29. H5 - Interactive versus infographic: phishing test score

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Score on phishing test (continuous)							
Infographic (reference)	**282**	**0.69**					
Interactive	**284**	**0.74**	**0.044**	**0.008**	**0.081**	**0.017**	**0.154**
Scored all correct on phishing test (binary)							
Infographic (reference)	282	27%					
Interactive	284	33%	0.062	-0.013	0.137	0.105	N.A.

Table 30. H5 - Interactive versus infographic: intention to update software

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Strong intention to update software (binary)							
Infographic (reference)	**280**	**88%**					
Interactive	**285**	**83%**	**-0.052**	**-0.106**	**0.001**	**0.055**	**0.491**
Likert score on intention to update software (continuous, 0-3 scale)							
Infographic (reference)	280	2.83					
Interactive	285	2.75	-0.086	-0.170	-0.001	0.048	N.A.

Table 31. H5 - Interactive versus infographic: intention to back up data

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)	p-value (bonferroni corrected)
Strong intention to back up data (binary)							
Infographic (reference)	**281**	**87%**					
Interactive	**286**	**88%**	**0.002**	**-0.046**	**0.050**	**0.937**	**1.0**
Likert score on intention to back up data (continuous, 0-3 scale)							
Infographic (reference)	281	2.83					
Interactive	286	2.82	-0.011	-0.080	0.058	0.753	N.A.

Survey questions

Cyber security survey for small businesses

Participant Information Sheet

This survey will take about 9 minutes to complete, and can be done on your mobile phone or computer.

The survey is being conducted by the Australian Cyber Security Centre to help make Australia the safest place to connect online.

Your responses will be used by the Australian Government to understand small businesses' awareness of, and resilience to, cyber security threats. The information you provide will help us improve our advice to small businesses. To support this work, your survey responses are collected using Qualtrics and stored onshore in Australia.

Your participation in this survey is voluntary, and you can stop at any time. If you stop, please know your responses will still be recorded and analysed. There will be no negative consequences if you choose not to participate, or if you stop participating once you've started.

Your responses will be kept anonymous. Results will be analysed and reported at an aggregate level.

Research approval for the survey has been cleared in accordance with the National Health and Medical Research Council's National Statement on Ethical Conduct in Human Research.

If you consent to participate, please proceed with the survey.

If you have any questions or concerns about this survey please contact the Australian Cyber Security Centre at ACSC.Small.Business@defence.gov.au

Please select the option that best describes your business' industry/sector

- ○ Agriculture, Forestry and Fishing
- ○ Mining
- ○ Manufacturing
- ○ Electricity, Gas, Water and Waste Services
- ○ Construction
- ○ Wholesale Trade
- ○ Retail Trade
- ○ Accommodation and Food Services
- ○ Transport, Postal and Warehousing
- ○ Information Media and Telecommunications
- ○ Financial and Insurance Services
- ○ Rental, Hiring and Real Estate Services
- ○ Professional, Scientific and Technical Services
- ○ Administrative and Support Services
- ○ Public Administration and Safety
- ○ Education and Training
- ○ Health Care and Social Assistance
- ○ Arts and Recreation Services
- ○ Other Services

Which occupation best describes your role in the business?

- ○ Business owner / manager
- ○ IT Professional
- ○ Professional
- ○ Technician and/or Trades Worker
- ○ Community and/or Personal Service Worker
- ○ Clerical and/or Administrative Worker
- ○ Sales Worker
- ○ Machinery Operator and/or Driver
- ○ Labourer
- ○ Other

Who is responsible for day to day management of IT security for your business?
Select all that apply:

- ○ Me
- ○ Another employee
- ○ An employee of the business dedicated to IT
- ○ Outsourced to an IT firm
- ○ Family or friend
- ○ Other
- ○ No-one

Which state/territory is your business registered in?

- ○ ACT
- ○ NSW
- ○ NT
- ○ QLD
- ○ SA
- ○ TAS
- ○ VIC
- ○ WA
- ○ Other

How many people does your business employ on a regular basis (including casual staff and business owner)?

- ○ 1 [I am self-employed/a sole trader]
- ○ 2 - 4
- ○ 5 - 19
- ○ 20 – 199
- ○ 200 +

What was the gross income for your business in the last financial year?(the income before paying tax)

- ○ Less than $50,000
- ○ $50,000 – $249,999
- ○ $250,000 – $499,999
- ○ $500,000 – less than $1 million
- ○ $1 million – less than $3 million
- ○ $3 million +
- ○ Prefer not to disclose

How do your clients or stakeholders communicate or engage with your business? Select all that apply:

- ○ At your office/shopfront/physical location
- ○ Via email
- ○ Via ecommerce website
- ○ Via telephone or VOIP
- ○ Via website
- ○ Via a portal
- ○ Via social media
- ○ Other

Which of the following computer devices does your business use during your day-to-day business operations? Select all that apply:

- ○ Windows desktop computer
- ○ Windows laptop computer
- ○ Apple desktop computer
- ○ Apple laptop computer
- ○ Linux desktop or laptop computer
- ○ None of these

Which of the following Windows operating system versions does your business currently use?

- ○ Windows 10
- ○ Windows 8 or 8.1
- ○ Windows 7
- ○ Windows Vista
- ○ Windows XP
- ○ ⊗Unsure

Which of the following Apple operating system versions does your business currently use?

- ○ Mojave
- ○ High Sierra
- ○ Sierra
- ○ El Capitan
- ○ Yosemite
- ○ Mavericks
- ○ Mountain Lion or Lion
- ○ Snow Leopard or Leopard
- ○ An older version
- ○ ⊗Unsure

When was the last time you bought new desktops or laptops for your business?

- ○ Less than 1 year ago
- ○ Between 1 and 3 years ago
- ○ Between 4 and 6 years ago
- ○ Between 7 and 10 years ago
- ○ Eleven or more years ago
- ○ Unsure

When was the last time you bought new Windows desktops or laptops for your business?

- ○ Less than 1 year ago
- ○ Between 1 and 3 years ago
- ○ Between 4 and 6 years ago
- ○ Between 7 and 10 years ago
- ○ Eleven or more years ago
- ○ Unsure

When was the last time you bought new Apple desktops or laptops for your business?

- ○ Less than 1 year ago
- ○ Between 1 and 3 years ago
- ○ Between 4 and 6 years ago
- ○ Between 7 and 10 years ago
- ○ Eleven or more years ago
- ○ Unsure

Which of the following portable smart devices does your business use during your day-to-day business operations? Select all that apply:

- ○ iPhone
- ○ iPad
- ○ Android phone
- ○ Android tablet
- ○ Windows phone
- ○ Windows tablet
- ○ Other phone
- ○ Other tablet
- ○ ⊗None of these

What other devices does your business use during your day-to-day business operations? Select all that apply:

- ○ Point Of Sale (POS) Terminals
- ○ Authentication tokens (two factor authentication)
- ○ EFTPOS Machine
- ○ Other device
- ○ ⊗None

What software does your business use during your day-to-day business operations? Select all that apply:

- ○ Anti-Virus software
- ○ Microsoft Office (e.g. Outlook, Word, Excel)
- ○ Internet browsers (e.g. Internet Explorer, Chrome, Firefox)
- ○ Accounting software (e.g. MYOB, Xero, Quickbooks)
- ○ Point of Sale software
- ○ Online based programs (e.g. Gmail, Hotmail)
- ○ Customer Relationship Management (CRM)
- ○ Password manager
- ○ ⊗None
- ○ Other (please specify below)

_____

Which of the following support services, if any, do you outsource as a part of your day-to-day business? Select all that apply:

- ○ General IT Support
- ○ Call centre/Customer service support
- ○ Offsite storage (e.g. Cloud storage)
- ○ Financial services/payroll
- ○ IT Security
- ○ ⊗None

Please indicate on the scale below how you would rate your understanding of cyber security:

- ○ **Expert** understanding
- ○ **Above average** understanding
- ○ **Average** understanding
- ○ **Some** understanding
- ○ **No** understanding

Please indicate on the scale below how important you believe cyber security is to your business:

- ○ **Very** important
- ○ **Somewhat** important
- ○ **Neither** important nor unimportant
- ○ **Somewhat** unimportant
- ○ **Not at all** important

Please indicate on the scale below how important you believe physical security is to your business:

- ○ **Very** important
- ○ **Somewhat** important
- ○ **Neither** important nor unimportant
- ○ **Somewhat** unimportant
- ○ **Not at all** important

Which of the following cyber security terms are you comfortable explaining to your staff or customers? (Yes/No)

- Malware
- Man–in-the-middle attack
- Spear phishing
- Trojan
- Ransomware
- Drive-by download
- Phishing
- Key logger
- Insider threat

Which of the following cyber security practices are applied in your business? (Yes/No)

- Application Whitelisting
- Patching Applications
- Application hardening
- Restricting admin access
- Disabling Macros
- Turning on multi-factor authentication
- Daily Backups
- Patching Operating systems

Has your business ever encountered a cyber security incident?
Examples of cyber incidents include, but are not limited to:

- Being subject to an online scam – e.g. Fake and/or malicious invoices, emails or messages
- Infection of your business systems or machines by malware, viruses or spyware
- Unauthorized access to your work systems, email or accounts by either staff or unknown parties

○ Yes, my business has experienced one or more cyber incidents
○ No, my business has not experienced a cyber incident

You selected, "Yes, my business has experienced one or more cyber incidents" - What happened?
Please provide a brief description: [_____]

What do you believe is the likelihood your business will encounter a cyber security incident in the next 12 months?

Examples of cyber incidents include, but are not limited to:

- Being subject to an online scam – e.g. Fake and/or malicious invoices, emails or messages
- Infection of your business systems or machines by malware, viruses or spyware
- Unauthorized access to your work systems, email or accounts by either staff or unknown parties

- ○ Almost certain
- ○ Likely
- ○ Possible
- ○ Unlikely
- ○ Highly unlikely
- ○ Don't know

If your business lost access to all of your critical data and systems, how soon do you think your business could regain business-as-normal operations?

- Immediately – I have Backups and other measures in place that would make recovery easy
- A few days – either myself or my service provider would be able to get the business back up and running
- A few weeks – the damage would be considerable but my business systems would be recoverable
- Never – my business would never be able to recover
- Unsure

Approximately how much does your business spend per year on cyber security?
This includes but is not limited to money spent on external IT security providers, cyber security software or services and IT staff.

- ○ Less than $500
- ○ $500 - $999
- ○ $1,000 – $4,999
- ○ $5,000 – $9,999
- ○ $10,000 - $49,999
- ○ $50,000 or more
- ○ Unsure

How do you prefer to receive information about cyber security for your business? Please choose your top 3 from the following list:

- ○ Email
- ○ Government website
- ○ Online newsletter
- ○ Trusted adviser (e.g. your accountant)
- ○ Telecommunications provider (e.g. Telstra)
- ○ Google
- ○ Other internet search engines
- ○ IT professional
- ○ Family/Friends
- ○ Business or industry associations
- ○ Twitter
- ○ Facebook
- ○ LinkedIn
- ○ Do not require this information

Your online activities Please tell us what you do when you are online.

If an email comes from someone I know, I don't always click on the link.

- ○ Strongly disagree
- ○ Disagree
- ○ Neither agree nor disagree
- ○ Agree
- ○ Strongly agree

If an email from an unknown sender looks interesting, I click on the link.

- ○ Strongly disagree
- ○ Disagree
- ○ Neither agree nor disagree
- ○ Agree
- ○ Strongly agree

I don’t open email attachments if I don’t know the sender.

- ○ Strongly disagree
- ○ Disagree
- ○ Neither agree nor disagree
- ○ Agree
- ○ Strongly agree

To your knowledge, have you ever clicked on a link in an email or text from an unknown sender?

- ○ Yes, in the last six months
- ○ Yes, but not recently
- ○ No, I don't think so

To your knowledge, have you ever replied to a phishing email (scam email)?

- ○ Yes, in the last six months
- ○ Yes, but not recently
- ○ No, I don't think so

Does your business install software updates?

- ○ Yes, updates are installed automatically
- ○ Yes, frequently
- ○ Yes, usually
- ○ Sometimes
- ○ Not usually
- ○ Not at all
- ○ Not to my knowledge

Does your business back up information on all devices (or store in the cloud)?

- ○ Yes, system backs up automatically
- ○ Yes, frequently
- ○ Yes, usually
- ○ Sometimes
- ○ Not usually
- ○ Not at all
- ○ Not to my knowledge

Nearly done! We just have a few more questions, and some suggestions that we hope will be helpful in future.

Thinking about the next seven days, how likely are you to check for software updates on your business devices?

- ○ System is already in place
- ○ Definitely
- ○ Likely
- ○ Unlikely
- ○ Definitely not

Thinking about the next seven days, how likely are you to initiate regular backups of business data?

- ○ System is already in place
- ○ Definitely
- ○ Likely
- ○ Unlikely
- ○ Definitely not

We've prepared this short 'starting steps' guide of key cyber security actions that your business can take to strengthen your cyber resilience.

Would you find this guide useful in your business?

- ○ Yes
- ○ No

Would you like to save a copy for yourself? (This is not a test!)

- ○ Save a copy for yourself
- ○ No thanks, take me to the end of the survey

Download the PDF of the guide here **and save to your device. Or, screen capture it. (This is not a test!)**

Thank you for taking the time to complete this survey.

If you would like to report a cyber security incident, please go to https://www.cyber.gov.au/report. If you have experienced a cyber incident and would like to talk about it with someone, IDCARE specialises in providing support to individuals and businesses. You can visit their website https://www.idcare.org or call them on AU: 1300 432 273.

Your responses provide valuable insights, and will help support the work of the Australian Cyber Security Centre (ACSC).

If you have any questions or concerns about this survey please contact The Australian Cyber Security Centre

Clicking NEXT will submit the survey and redirect you to the Australian Cyber Security Centre Website.

Cyber survey for small businesses - Follow up survey

Which of the following cyber security practices have you adopted in your business in the last 3 or 4 weeks? (i.e. since completing the previous ACSC cyber security survey)
Select all that apply:

- ○ Application Whitelisting
- ○ Patching Applications
- ○ Application hardening
- ○ Restricting admin access
- ○ Disabling Macros
- ○ Turning on multi-factor authentication
- ○ Daily Backups
- ○ Patching Operating systems
- ○ None of the above

What motivated you to adopt these cyber security practices?
[_____}

Does your business install software updates?

- ○ Yes, updates are installed automatically
- ○ Yes, frequently
- ○ Yes, usually
- ○ Sometimes
- ○ Not usually
- ○ Not at all
- ○ Not to my knowledge

Does your business back up information on all devices (or store in the cloud)?

- ○ Yes, system backs up automatically
- ○ Yes, frequently
- ○ Yes, usually
- ○ Sometimes
- ○ Not usually
- ○ Not at all
- ○ Not to my knowledge

Your online activities Please tell us what you do when you are online.

If an email comes from someone I know, I don't always click on the link.

- ○ Strongly disagree
- ○ Disagree
- ○ Neither agree nor disagree
- ○ Agree
- ○ Strongly agree

If an email from an unknown sender looks interesting, I click on the link.

- ○ Strongly disagree
- ○ Disagre
- ○ Neither agree nor disagree
- ○ Agree
- ○ Strongly agree

I don't open email attachments if I don't know the sender.

- ○ Strongly disagree
- ○ Disagree
- ○ Neither agree nor disagree
- ○ Agree
- ○ Strongly agree

Do you remember this 'starting steps' guide of key cyber security actions that your business can take to strengthen your cyber resilience?

- ○ Yes
- ○ No

Did you download a copy of the guide?

- ○ Yes I printed it
- ○ Yes, downloaded but didn't print it
- ○ No

[if yes] Did you try to use the guide (or use elements of it)?

- ○ Yes
- ○ No

[if yes] Did you find the guide useful in your business?

- ○ No, not at all
- ○ Not very useful
- ○ Unsure
- ○ Somewhat useful
- ○ Very useful (5)

Which elements of the guide were useful or not useful? How did you use it in your business? [_____]

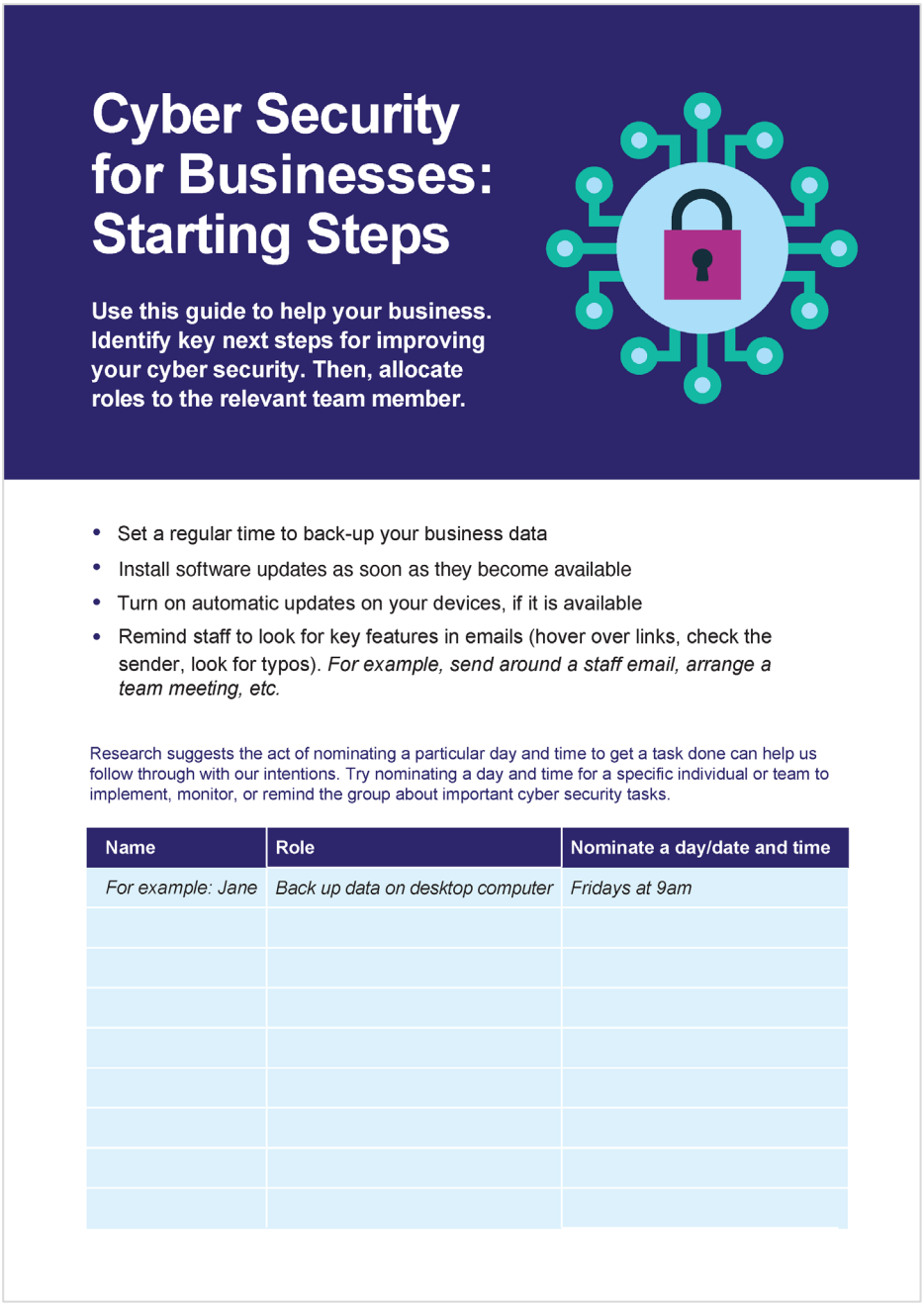
[if no] Why didn't you use the guide?

- ○ My business already does all the recommended actions
- ○ I forgot about it
- ○ I have been too busy
- ○ Not practical
- ○ Other (please specify) [_____]

Click NEXT to submit the survey

Please note that final submission of the entire survey implies formal consent to participate in this research activity.

Starting Steps guide



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*

Figure 7: Starting Steps guide to cyber security for businesses

Cyber security survey of individuals

Focus groups

Methodology

BETA commissioned ChatHouse to facilitate focus groups with individuals. ChatHouse conducted four focus groups across two urban and two regional locations: Ballarat and Melbourne in Victoria, and Wollongong and Sydney in New South Wales. The research took place on 30 September and 1 October 2019. Each session lasted two hours, with groups ranging between seven and eight people per group.

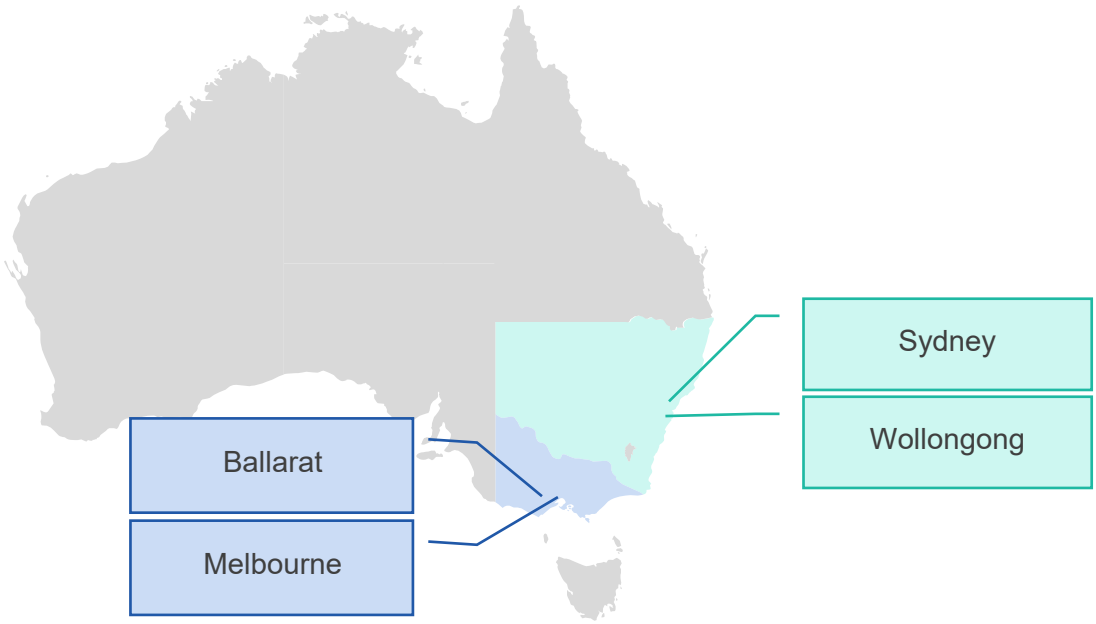


Figure 8: Locations of focus groups

We chose to split groups across urban and regional areas to get a better spread of participants. We also included one group of participants from lower socioeconomic backgrounds. Groups were open to participants aged between 20 and 65 years. We sought to include a good spread of ages because we believe awareness of and practice in cyber security differs across generations. We also sought to have an even split between male and

female participants, and to include some participants from Culturally and Linguistically Diverse (CALD) backgrounds.

Table 32. Demographics of focus groups

Group	1	2	3	4
Location	Sydney	Wollongong	Melbourne	Ballarat
Age range	20-65 years	20-65 years	20-65 years	20-65 years
Income status	Not specified	Not specified	Low income	Not specified

Participants were recruited through a third party recruitment company. People were excluded if, in the initial screening questions, they:

- Reject the notion of cyber security (as an issue)
- Were not open to hearing messages about cyber security
- Had exceptionally high cyber security practices already
- Exclusively use internet enabled devices they don't own

We asked participants about their current attitudes, knowledge and behaviours related to cyber security. In particular, we focused on the barriers and drivers people perceived when it came to their cyber security. We also asked them to review some mocked up advice with different designs and behavioural concepts and indicate which parts, if any, they found most compelling or credible (and if not, why not).

Results

ChatHouse provided a final report summarising the key themes across all four groups:

Participants were overloaded and focused on daily priorities

- New and complex passwords are too hard to remember, especially when passwords are required across so many accounts and devices.
- Software updates interrupt people when they are using their devices, prompting people to 'snooze' notifications or ignore them altogether.

Participants relied too much on companies, banks, or governments to keep them secure online, rather than taking personal responsibility

- Many perceived cyber security to be less of an individual responsibility and more the responsibility of large companies that have the capacity to safeguard their sites, devices, and accounts.
- When prompted, many also believe Government has an important role in cyber security, especially in relaying advice or guidance.

- Personal responsibility is further undermined by a degree of fatalism born out of a recognition it is impossible to be entirely secure.

Participants underestimated their vulnerability to threats

- Their own perceived ‘ordinariness’ is felt to make individuals less vulnerable to threats (e.g. ‘I don’t have anything worth seeing/stealing’).
- Some responses seemed in line with the ‘congruence heuristic’—because an incident had not happened to them in the past, they were more inclined to assume it would not (or was less likely to) happen in the future.
- Some participants expressed attitudes linked with ‘self-serving attribution bias’—attributing not having had issues in the past to their inherent common sense and ability to detect scams.
- There were some misconceptions that secure systems at a corporate level safeguard individuals at a local level.
- Participants underestimated the potential consequences of a security breach, assuming most problems to be easily fixed (e.g. banks return money).

Technical details

Overview of the survey experiment for individuals

In partnership with the Australian Cyber Security Centre (ACSC), we conducted research to improve cyber security advice for individuals in their personal lives.

The study involved a survey and, embedded within that, two survey experiments. The survey itself studied attitudes towards and awareness of cyber security, as well as the current cyber security practices of Australians. The embedded survey experiments examined whether different ways of presenting information—varying the messenger or the consequences of inaction—might change behavioural intentions, or actual behaviours. The first experiment presented information about password security, the second about software updates

All participants received a follow-up survey, which assessed self-reported behavioural change for password security and software updates. Both the initial and follow-up surveys were conducted through an online survey platform with Australian Survey Research. The initial survey had a sample size of 4,489 respondents.

The project was approved through BETA's ethics approval process, with risk assessed in accordance with the guidelines outlined in the National Statement on Ethical Conduct in Human Research. It was reviewed by a delegate committee in accordance with the National Statement and assessed as low risk.

Pre-registration and pre-analysis plan

The survey ran from 3 March to 3 April 2020. We pre-registered on the American Economic Association RCT Registry (RCT ID no. AEARCTR-0005519) under the title 'Using websites effectively for sharing cyber security advice' on 2 March 2020. The pre-analysis plan was uploaded on 6 April 2020 after trial completion but before receipt of any data.

There were no deviations from our pre-analysis plan. However, covariate data was missing for a small number of respondents and we had not pre-specified how we would address this in our analysis. We discuss this further in the Missing Data section below.

Interventions

For each experiment, we tested two sets of interventions varying: the messenger, and how the consequences of suboptimal behaviour were framed. Each trial therefore used a 2x3 factorial design.

- Messenger: The advice came from a 'peer' messenger, or an 'expert' messenger, or no messenger (attention control).
- Consequences (financial/non-financial): The consequences of suboptimal cyber security behaviour were framed around either the financial gains and losses or the impact on other aspects of their lives.

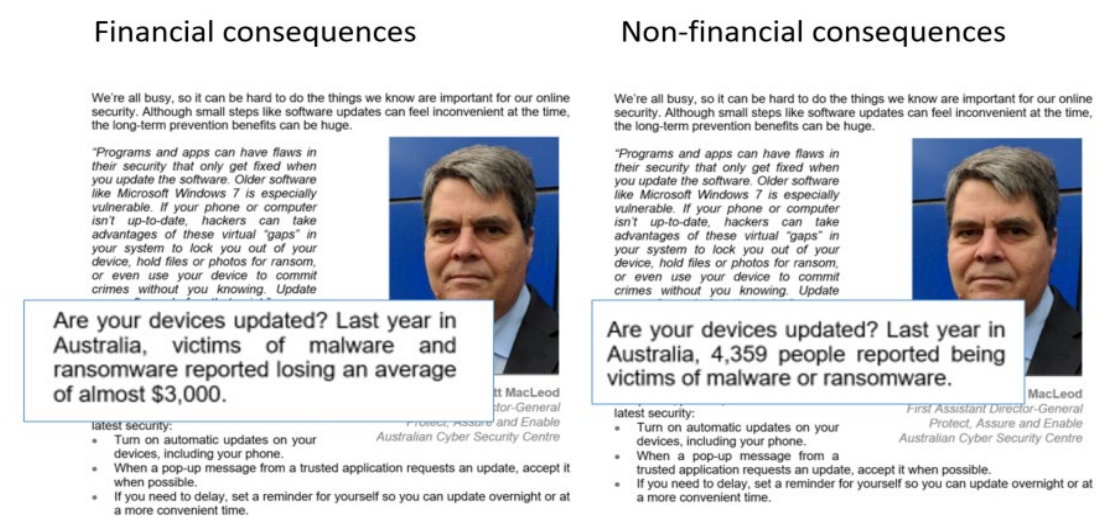


Figure 9: Consequences: examples of financial or non-financial consequences

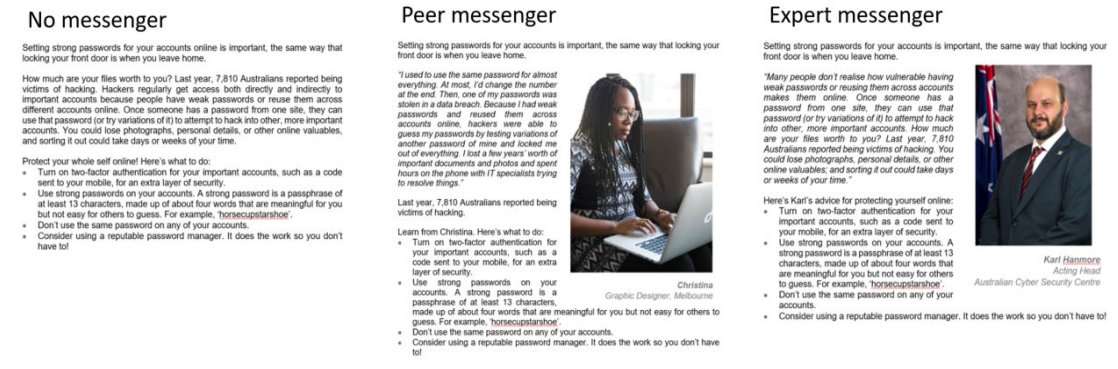


Figure 10: Messenger: examples of peer messenger, expert messenger, or no messenger

Outcomes

For each experiment there were four primary outcomes (both for password security and for software updates):

Primary outcome 1—Knowledge (at the time of exposure)

Primary outcome 2—Knowledge (three weeks later)

Primary outcome 3—Self-reported behavioural intentions (at the time of exposure)

Primary outcome 4—Self-reported behaviours (three weeks later)

The details of how each outcome was measured are set out in the following tables.

Table 33. Outcome measures: password security

Outcome measure	Question	Response options
Knowledge at exposure: main survey (Only used the answer for the second password (the passphrase)).	How do you rate the strength of these passwords? (password1, **fieldhayfaretoss**, wjh63m&92mk11gr9)	1. Very strong 1. Strong 0. Weak 0. Very weak
Knowledge three weeks later: follow-up survey (We only used the answer for the second password (the passphrase)).	How do you rate the strength of these passwords? (Tuesday25, **trendagepairdeer**, n8j2n3wzhz3edygs)	1. Very strong 1. Strong 0. Weak 0. Very weak
Self-reported behavioural intentions: main survey (Indexed from summing the responses to the two questions, each on a 0-4 scale, giving a maximum possible score of 8.	How likely are you to create **strong** passwords for your important accounts (such as your online banking, email, and social media accounts)? How likely are you to create **different** passwords for your important accounts (such as your online banking, email, and social media accounts)?	4. Extremely likely 3. Very likely 2. Moderately likely 1. Somewhat likely 0. Not at all likely
Self-reported behaviours: follow-up survey (Indexed from summing the responses to the two questions, each on a 0-3 scale, giving a maximum possible score of 6.)	In the last three weeks, did you create **strong** passwords across your important accounts (such as your online banking, email, and social media accounts)? In the last three weeks, did you create **different** passwords across your important accounts (such as your online banking, email, and social media accounts)?	3. Yes for ALL of my important accounts 2. Yes for MOST of my important accounts 1. Yes for SOME of my important accounts 0. No

Table 34. Outcome measures: software updates

Outcome measure	Question	Response options
Knowledge at exposure: main survey (This is treated as binary, with the final option coded as 'correct'.)	When you receive a notification to update software on your personal device, does it matter how soon you update it? Select the best answer:	0. No, as long as you update eventually 0. No, as long as you update within a week 0. Yes, you need to update it within 24 hours 1. Yes, the longer you wait the more vulnerable you are
Knowledge 3 weeks later: follow-up survey	When you receive a notification to update software on your personal device, does it matter how soon you update it? Select the best answer:	0. No, as long as you update eventually 0. No, as long as you update within a week 0. Yes, you need to update it within 24 hours 1. Yes, the longer you wait the more vulnerable you are
Self-reported behavioural intentions: main survey (We treated this variable as continuous.)	When prompted on a personal device, how likely are you to update the software immediately?	4. Extremely likely 3. Very likely 2. Moderately likely 1. Somewhat likely 0. Not at all likely
Self-reported behaviours: follow-up survey (We treated this variable as continuous. People who did not receive a notification in the last three weeks were coded as 0, the same as 'Haven't done the update yet')	How long after you got the update notification did you do the update? (If you got more than one update, think of the last one you received.)	4. Immediately 3. Within 2 days 2. Within 7 days 1. More than 7 days later 0. Haven't done the update yet

Hypotheses

Since the interventions for both experiments (password security and software updates) had the same structure, we also had the same hypotheses for each of the four outcome measures (knowledge and intention, for passwords and updates). As indicated below, directional hypotheses were tested using a one-sided test; non-directional hypotheses were tested using a two-sided test.

H1a-H1d: The four outcomes will be higher among respondents exposed to ***any*** *messenger* (pooled) compared to the *attention control* (one-sided test).

H2a-H2d: The four outcomes will be higher among respondents exposed to ***each*** *messenger* compared to the *attention control* (one-sided test).

H3a-H3d: The four outcomes will be different among respondents exposed to the *peer messenger* compared to the *expert messenger* (two-sided test).

H4a-H4d: The four outcomes will be different among respondents exposed to the *financial consequences* condition compared to the *non-financial consequences* (two-sided test).

Study population, sample size and randomisation

Participants were recruited through Australian Survey Research, who endeavoured to ensure that the sample was representative of the larger Australian population. To ensure balance across age, gender, and location, potential respondents declared their gender, age bracket, and state, before they were permitted into the survey. If the quota for their age+gender+state was filled, they were unable to proceed with the survey. For those who did complete the survey, this initial demographic information was included in their response data. In order to achieve our desired sample size, we relaxed the state quotas part way through the data collection period.

As noted above, both experiments had a 2x3 factorial design. The first experiment presented advice on password security, the second on software updates. In each experiment, all participants were randomised into one one of six possible cells based on a combination of: two variations in the consequences, and three messenger arms.

Table 35. Number of participants randomised into each treatment cell

Experiment	Consequence	Attn. Control	Expert	Peer
Password security	**Financial** N = 2,247	**A1** n = 715	**A2** n = 783	**A3** n = 749
	Non-financial N = 2,242	**A4** n = 784	**A5** n = 758	**A6** n = 700
	Sub-totals	**Attn. Control** N = 1,499	**Expert** N = 1,541	**Peer** N = 1,449
Software updates	**Financial** N = 2,267	**B1** n = 746	**B2** n = 781	**B3** n = 740
	Non-financial N = 2,222	**B4** n = 729	**B5** n = 719	**B6** n = 774
	Sub-totals	**Attn. Control** N = 1,475	**Expert** N = 1,500	**Peer** N = 1,514

Sample frame: N = 4,489, deterministic, participants randomised at an individual level and sorted into one of 36 possible pathways

Participants were initially randomised at an individual level for allocation to the password security experiment (cells A1 through A6 in). All participants were then re-randomised to the software update experiment (cells B1 through B6). Randomisation into B1 through B6 was blocked on randomisation to A1 through A6.

Randomisation took place in advance using a larger sample frame of 20,000 participants, but data collection ended once 4,500 responses were collected. We didn't have control which 4,500 people would respond, so although randomisation was set up to deliver about 750 individuals per cell, the exact numbers varied around this average.

We had a high retention rate for the follow-up survey three weeks later: 73 per cent of the original sample frame responded (Table 36).

Table 36. Retention rate at follow-up, three weeks later

Experiment	Consequence	Attn. Control	Expert	Peer
Password security	**Financial** N = 1,621	**A1** n = 503	**A2** n = 562	**A3** n = 556
	Non-financial N = 1,640	**A4** n = 558	**A5** n = 573	**A6** n = 509
	Sub-totals	**Attn. Control** N = 1,061	**Expert** N = 1,135	**Peer** N = 1,065
Software updates	**Financial** N = 1,636	**B1** n = 537	**B2** n = 565	**B3** n = 534
	Non-financial N = 1,625	**B4** n = 520	**B5** n = 541	**B6** n = 564
	Sub-totals	**Attn. Control** N = 1,057	**Expert** N = 1,106	**Peer** N = 1,098

Sample frame at follow-up survey, three weeks later (N = 3,261, 73% retention rate)

Power calculations

Our power calculations assumed we would have sample of 4,500. We calculated the following minimum detectable effect sizes based on an alpha of 0.05 and 80% power. (Note: these analyses are for the intervention at exposure, because three weeks later the sample was smaller due to attrition.)

Table 37. Minimum detectable effect

Messenger (H1a-d & H2a-d, one-sided) N = 1,500 per group	Messenger (H3a-d, two-sided) N = 1,500 per group	Financial (H4a-d, two-sided) N = 2,250 per group
9%	10%	8%

Power = 0.8, alpha = 0.05

Method of analysis

We used a linear regression model with the following specification for our primary analysis:

$$Y = a + b1T1 + b2T2a + b3T2b + b4X + b5XT1 + b6XT2a + b7XT2b + e$$

Where Y is an outcome variable, T1 is a dummy variable for financial consequences, T2a is a dummy variable for the peer messenger, T2b is a dummy variable for the expert messenger, and X is a vector of mean-centred covariates, which were interacted with each of the treatment dummies.

We also conducted a robustness check for our binary outcomes by running a logistic regression and calculating average marginal effects.

Covariates

We included the following covariates in all estimation equations.

Table 38. List of covariates

Covariate	Response format
Reported frequency of installing software updates on the day they are released	4. Every time 3. Most of the time 2. Sometimes 1. Rarely 0. Never 0. Don't know
Reported frequency of using a **different** password for important accounts	
Reported frequency of using a **strong** password for important accounts	

Missing data

We did not have any missing outcome data from the main survey as the responses to outcome questions were mandatory. If the mandatory questions were not completed, that survey was discarded for the purposes of the survey experiment (though their responses to the survey were kept) and another respondent was recruited.

We did have missing data for the follow-up survey. Although respondents were compensated for their time, we had an attrition rate between the main survey and follow-up survey of around 27 per cent. We do not believe the form of treatment delivered in the main survey could have influenced respondents' subsequent decisions about whether to complete the follow-up survey, and we saw no evidence of imbalance in response rates. Consequently, we undertook complete case analysis (that is, we dropped the records with missing outcomes) and proceeded on the assumption that the dropped records were missing independent of potential outcomes (MIPO).

In a small number of cases we had missing covariate data: 14 missing values for *Update behaviours,* 11 missing values for *Using different passwords,* and 18 missing values for *Using strong passwords.* For these cases, we randomly sampled values from other respondents to replace the missing covariate values. We did not anticipate this in our pre-analysis plan and we faced a choice between imputing covariate values or dropping observations. We tried both and found that it had no material impact on our results.

Key statistical tables

Overview

This appendix presents the statistical analyses and robustness checks undertaken for the survey experiment within the Cyber security survey of individuals. For both parts of the experiment, we present the results for our four outcomes: binary outcome variables for knowledge at time of exposure, and knowledge three weeks later; and continuous outcome variables for intentions at time of exposure, and behaviours three weeks later.

The tables present the main effects for each of these outcomes for each hypothesis:

- H1: Messengers (pooled) versus attention control (Table 39 and Table 40).
- H2: Peer or expert messengers versus attention control (Table 41 and Table 42).
- H3: Peer messengers versus expert messengers (Table 43 and Table 44).
- H4: Financial versus non-financial consequences (Table 45 and Table 46).

Means, treatment effects, 95 per cent confidence intervals and p-values are from adjusted linear regression models (see Power = 0.8, alpha = 0.05

Method of analysis). The group sample size is n. One-sided hypotheses are presented with a single-sided confidence interval. Occasionally the difference in means is slightly different from the effect estimates: this is due to rounding error.

Table 39. H1 - Pooled messengers versus none: password security

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)
Knowledge at time of exposure (binary)						
Attention control	**1,501**	**0.767**				
Pooled messengers	**2,991**	**0.772**	**0.005**	**-0.017**	**N.A.**	**0.351**
Knowledge three weeks later (binary)						
Attention control	1,061	0.715				
Pooled messengers	2,200	0.724	0.009	-0.019	N.A.	0.301
Self-reported behavioural intentions at time of exposure (continuous)						
Attention control	**1,501**	**6.087**				
Pooled messengers	**2,991**	**6.037**	**-0.050**	**-0.131**	**N.A.**	**0.844**
Self-reported behaviours three weeks later (continuous)						
Attention control	1,059	2.620				
Pooled messengers	2,191	2.599	-0.021	-0.151	N.A.	0.604

Table 40. H1 - Pooled messengers versus none: software update

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)
Knowledge at time of exposure (binary)						
Attention control	1,477	0.480				
Pooled messengers	3,015	0.477	-0.003	-0.028	N.A.	0.567
Knowledge three weeks later (binary)						
Attention control	1,056	0.522				
Pooled messengers	2,202	0.488	-0.034	-0.064	N.A.	0.971
Self-reported behavioural intentions at time of exposure (continuous)						
Attention control	1,477	2.594				
Pooled messengers	3,015	2.649	0.056	0.003	N.A.	0.041
Self-reported behaviours three weeks later (continuous)						
Attention control	1,052	1.561				
Pooled messengers	2,199	1.544	-0.017	-0.122	N.A.	0.606

Table 41. H2 - Expert and peer messengers versus none: password security

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)
Knowledge at time of exposure (binary)						
Attention control (reference)	**1,501**	**0.767**				
Expert messenger	**1,541**	**0.775**	**0.008**	**-0.017**	**N.A.**	**0.299**
Peer messenger	**1,450**	**0.769**	**0.002**	**-0.024**	**N.A.**	**0.460**
Knowledge three weeks later (binary)						
Attention control (reference)	1,061	0.715				
Expert messenger	1,135	0.718	0.003	-0.029	N.A.	0.445
Peer messenger	1,065	0.730	0.014	-0.018	N.A.	0.230
Self-reported behavioural intentions at time of exposure (continuous)						
Attention control (reference)	**1,501**	**6.087**				
Expert messenger	**1,541**	**6.033**	**-0.053**	**-0.145**	**N.A.**	**0.830**
Peer messenger	**1,450**	**6.040**	**-0.047**	**-0.142**	**N.A.**	**0.793**
Self-reported behaviours three weeks later (continuous)						
Attention control (reference)	1,059	2.620				
Expert messenger	1,131	2.585	-0.036	-0.185	N.A.	0.653
Peer messenger	1,060	2.617	-0.003	-0.155	N.A.	0.514

Table 42. H2 - Expert and peer messengers versus none: software updates

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (one-sided)
Knowledge at time of exposure (binary)						
Attention control (reference)	**1,477**	**0.480**				
Expert messenger	**1,501**	**0.478**	**-0.002**	**-0.031**	**N.A.**	**0.546**
Peer messenger	**1,514**	**0.476**	**-0.004**	**-0.033**	**N.A.**	**0.579**
Knowledge three weeks later (binary)						
Attention control (reference)	1,056	0.522				
Expert messenger	1,105	0.478	-0.044	-0.079	N.A.	0.983
Peer messenger	1,097	0.497	-0.025	-0.060	N.A.	0.886
Self-reported behavioural intentions at time of exposure (continous)						
Attention control (reference)	**1,477**	**2.594**				
Expert messenger	**1,501**	**2.658**	**0.064**	**0.004**	**N.A.**	**0.041**
Peer messenger	**1,514**	**2.641**	**0.047**	**-0.014**	**N.A.**	**0.101**
Self-reported behaviours three weeks later (continous)						
Attention control (reference)	1,052	1.561				
Expert messenger	1,104	1.526	-0.035	-0.156	N.A.	0.684
Peer messenger	1,095	1.561	0.000	-0.122	N.A.	0.502

Table 43. H3 - Peer versus expert messenger: password security

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (two-sided)
Knowledge at time of exposure (binary)						
Expert messenger (reference)	**1,541**	**0.775**				
Peer messenger	**1,450**	**0.768**	**-0.007**	**-0.037**	**0.023**	**0.652**
Knowledge three weeks later (binary)						
Expert messenger (reference)	1,135	0.718				
Peer messenger	1,065	0.729	0.011	-0.027	0.049	0.565
Self-reported behavioural intentions at time of exposure (continous)						
Expert messenger (reference)	**1,541**	**6.035**				
Peer messenger	**1,450**	**6.040**	**0.004**	**-0.106**	**0.114**	**0.940**
Self-reported behaviours three weeks later (continous)						
Expert messenger (reference)	1,131	2.585				
Peer messenger	1,060	2.616	0.031	-0.150	0.212	0.735

Table 44. H3 - Peer versus expert messenger: software updates

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (two-sided)
Knowledge at time of exposure (binary)						
Expert messenger (reference)	**1,501**	**0.479**				
Peer messenger	**1,514**	**0.477**	**-0.001**	**-0.036**	**0.033**	**0.938**
Knowledge three weeks later (binary)						
Expert messenger (reference)	1,105	0.480				
Peer messenger	1,097	0.499	0.019	-0.022	0.060	0.358
Self-reported behavioural intentions at time of exposure (continous)						
Expert messenger (reference)	**1,501**	**2.661**				
Peer messenger	**1,514**	**2.644**	**-0.016**	**-0.089**	**0.056**	**0.658**
Self-reported behaviours three weeks later (continous)						
Expert messenger (reference)	1,104	1.529				
Peer messenger	1,095	1.567	0.038	-0.105	0.180	0.604

Table 45. H4 - Financial versus non-financial consequences: password security

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (two-sided)
Knowledge at time of exposure (binary)						
Non-financial consequences (reference)	**2,243**	**0.778**				
Financial consequences	**2,249**	**0.764**	**-0.014**	**-0.038**	**0.011**	**0.280**
Knowledge three weeks later (binary)						
Non-financial consequences (reference)	1,640	0.721				
Financial consequences	1,621	0.720	-0.001	-0.032	0.030	0.938
Self-reported behavioural intentions at time of exposure (continous)						
Non-financial consequences (reference)	**2,243**	**6.088**				
Financial consequences	**2,249**	**6.019**	**-0.068**	**-0.158**	**0.022**	**0.140**
Self-reported behaviours three weeks later (continous)						
Non-financial consequences (reference)	1,633	2.597				
Financial consequences	1,617	2.614	0.018	-0.129	0.164	0.812

Table 46. H4 - Financial versus non-financial consequences: software updates

Treatment group	*n*	Mean	Effect (relative to reference)	95% Confidence Interval		p-value (two-sided)
Knowledge at time of exposure (binary)						
Non-financial consequences (reference)	**2,223**	**0.473**				
Financial consequences	**2,269**	**0.483**	**0.010**	**-0.018**	**0.039**	**0.480**
Knowledge three weeks later (binary)						
Non-financial consequences (reference)	1,622	0.507				
Financial consequences	1,636	0.491	-0.016	-0.049	0.018	0.354
Self-reported behavioural intentions at time of exposure (continous)						
Non-financial consequences (reference)	**2,223**	**2.636**				
Financial consequences	**2,269**	**2.625**	**-0.012**	**-0.071**	**0.047**	**0.695**
Self-reported behaviours three weeks later (continous)						
Non-financial consequences (reference)	1,618	1.538				
Financial consequences	1,633	1.563	0.026	-0.091	0.143	0.667

Survey questions

Cyber security survey of individuals

Participation Information Sheet

The Australian Cyber Security Centre leads the Australian Government's efforts to improve Australia's digital security. The Centre's role is to help make Australia the safest place to connect online.

The information you provide will help us improve our cyber security advice to all Australians.

The survey will take about 15 minutes to complete and can be completed on any device connected to the internet. Your participation in the survey is voluntary. Dynata and the research company conducting the survey will keep your responses confidential. Dynata's privacy policy is here.

The information you and others provide through this survey will be analysed and reported at an aggregate (group) level. The Government will write research reports on the results, but these reports will not include information that could identify you or other people that participate in the survey.

If you have any questions, please contact Dynata here.

Click *Next* below to start answering.

Last week, did you have a job of any kind?

A job means any type of work including casual, temporary, part-time or full-time work, and it was for one hour or more.

- ☐ Yes - worked for payment or profit
- ☐ Yes - but absent on paid or unpaid leave, on strike, or temporarily stood down
- ☐ Yes - unpaid work in a family business
- ☐ Yes - other unpaid work
- ☐ No - I did not have a job last week

How many people work in your workplace?

When answering, think about the place where you work, not the whole organisation.

- ☐ No other employees (other than owner/s)
- ☐ 1 to 19 employees
- ☐ 20 or more employees

How much do you think you know about digital security?

- ☐ A lot
- ☐ A fair bit
- ☐ A little bit
- ☐ Nothing or very little

How many people work in your workplace?

When answering, think about the place where you work, not the whole organisation.

- ☐ No other employees (other than owner/s)

- ☐ 1 to 19 employees
- ☐ 20 or more employees

How much do you think you know about digital security?

- ☐ A lot
- ☐ A fair bit
- ☐ A little bit
- ☐ Nothing or very little

Thinking about your digital security, how **safe** are each of the following things?

	Extremely safe	Very safe	Moderately safe	A little safe	Not at all safe	Don't know
Clicking on links in emails from people I know	☐	☐	☐	☐	☐	☐
Sharing my passwords with my friends	☐	☐	☐	☐	☐	☐
Connecting to public Wi-Fi to do internet banking	☐	☐	☐	☐	☐	☐
Allowing public access to personal information (like my age and gender) on my social media accounts	☐	☐	☐	☐	☐	☐

Thinking about your digital security, how **useful** are each of the following?

	Extremely useful	Very useful	Moderately useful	A little useful	Not at all useful	Don't know
Using anti-virus software	☐	☐	☐	☐	☐	☐
Using a second layer of security on accounts (or two-factor authentication), such as a code sent to my mobile	☐	☐	☐	☐	☐	☐

Installing software updates on my devices	☐	☐	☐	☐	☐	☐

Which of the following have you done in your personal life (not at work) in the last week?
Select all that apply

- ☐ Sent or received an email
- ☐ Looked at one or more websites
- ☐ Used social media (including reading, looking, posting, following, commenting or liking something)
- ☐ Accessed government services online (MyGov, Centrelink, etc.)
- ☐ Used internet banking, including banking apps (checked my balance, paid a bill, etc.)
- ☐ Online shopping
- ☐ Online gaming
- ☐ Used apps connected to data / Wi-Fi (Google maps, weather, news, etc.)
- ☐ Streamed or downloaded videos, movies, music etc. (Netflix, Spotify, etc.)
- ☐ Made telephone or video calls using Skype, WhatsApp, WeChat or similar
- ☐ Used a smart watch
- ☐ Used a digital home system (Alexa, Google Home, etc.)

How often do you do each of the following things in your personal life (not at work)?

	Every time	Most of the time	Sometimes	Rarely	Never	Don't know
I install the latest software and app updates the same day I get a notification to do so	☐	☐	☐	☐	☐	☐
I check emails, texts or social media messages to see whether they are scams	☐	☐	☐	☐	☐	☐
I back up my most important information (like files and photos)	☐	☐	☐	☐	☐	☐
I save passwords using a password manager	☐	☐	☐	☐	☐	☐
I use a different password for each of my most important accounts (such as my email, bank and social media accounts)	☐	☐	☐	☐	☐	☐
I use a strong password for each of my most important accounts (such as my email, bank and social media accounts)	☐	☐	☐	☐	☐	☐

	Every time	Most of the time	Sometimes	Rarely	Never	Don't know
I review the privacy settings on my social media accounts	☐	☐	☐	☐	☐	☐
I read the privacy statement when signing up to new online accounts	☐	☐	☐	☐	☐	☐

In the last month, how often have you done each of the following in your personal life?

	More than 5 times	3 to 4 times	Once or twice	Never	Not sure
Clicked on a link in an email from someone I did not know	☐	☐	☐	☐	☐
Used public Wi-Fi to do my internet banking	☐	☐	☐	☐	☐
Entered my bank or credit card details on a website that is not from a well-known company or brand	☐	☐	☐	☐	☐
Shared my passwords with my friends	☐	☐	☐	☐	☐
Ignored a notification to update my software	☐	☐	☐	☐	☐

Where do you get information about digital security?

Select all that apply

- ☐ Friends or family
- ☐ Workplace - colleagues (who are not IT staff) or employer
- ☐ Workplace - IT / computer / security staff
- ☐ Internet service provider (Telstra, Optus, TPG, etc.)
- ☐ Internet security software company (like an anti-virus supplier)
- ☐ Financial institutions (banks, insurance companies, superannuation funds, credit unions, etc)
- ☐ Government (the Australian Cyber Security Centre, eSafety Commissioner, Stay Smart Online, ScamWatch, the Police, etc.)
- ☐ The supplier (online or in-store) where I purchased my device (JB Hi-Fi, Bing Lee, Harvey Norman, Officeworks, etc)
- ☐ Online sources like forums / blogs / podcasts / websites / online articles
- ☐ Television, magazines, newspapers, radio
- ☐ The company that made my device (Apple, Hewlett Packard, Samsung, Dell, etc)
- ☐ I don’t seek out information on online security
- ☐ Other :Please specify_____

Of the sources you selected, which do you consider the most trustworthy source of advice?
Select one answer only

- ☐ Friends or family
- ☐ Workplace - colleagues (who are not IT staff) or employer
- ☐ Workplace - IT / computer / security staff
- ☐ Internet service provider (like Telstra, Optus, TPG, etc.)
- ☐ Internet security software company (like anti-virus supplier)
- ☐ Financial institutions (banks, insurance companies, superannuation funds, credit unions, etc)
- ☐ Government (the Australian Cyber Security Centre, eSafety Commissioner, Stay Smart Online, ScamWatch, the Police, etc.)
- ☐ The supplier (online or in-store) where I purchased my device (JB Hi-Fi, Bing Lee, Harvey Norman, Officeworks, etc)
- ☐ Online sources like forums / blogs / podcasts / websites / online articles
- ☐ Television, magazines, newspapers, radio
- ☐ The company that made my device (Apple, Hewlett Packard, Samsung, Dell, etc)
- ☐ Other

Have you experienced any of the following cyber incidents in your personal life?

	Yes, in the last 12 months	Yes, but more than 12 months ago	Don't know/unsure
Scam messages - I received a message that (tried to) trick me into giving money or personal information	☐	☐	☐
Malware or viruses - I got harmful software on my device that was designed it to slow it down, stop working or spy on me	☐	☐	☐
Ransomware - I was locked out of my computer, files or programs and was told to pay a fee to get it unlocked	☐	☐	☐
Hacking - My online account(s) was accessed without my permission	☐	☐	☐
Buying or selling scam - I made a payment or donation online, but something went wrong, like the product never arrived	☐	☐	☐
Identity theft - My identity was stolen or misused online	☐	☐	☐
Online harassment, cyberbullying, or online stalking - someone subjected me to online abuse	☐	☐	☐
Image-based abuse - My intimate photos or videos were shared online without my permission	☐	☐	☐

	Yes, in the last 12 months	Yes, but more than 12 months ago	Don't know/unsure
Dating fraud - My online romantic partner deceived me into giving them money or gifts	☐	☐	☐

Which of the incidents you selected in the previous question was the **most recent** incident?

- ☐ Scam messages
- ☐ Malware or viruses
- ☐ Ransomware
- ☐ Hacking
- ☐ Buying or selling scam
- ☐ Identity theft
- ☐ Online harassment, cyberbullying, r online stalking
- ☐ Image-based abuse
- ☐ Dating fraud

Thinking about this most recent [piped content] incident, who did you report the incident to?
Select all that apply

- ☐ No one
- ☐ Friends or family
- ☐ ID Care
- ☐ Colleagues / staff at my workplace who do not work in IT
- ☐ Colleagues / staff at my workplace who work in IT/ computers/ security
- ☐ Internet service provider (Telstra, Optus, TPG, etc.)
- ☐ Internet security software company (like anti-virus supplier)
- ☐ Financial institutions (banks, insurance companies, superannuation funds, credit unions, etc)
- ☐ Australian Cyber Security Centre
- ☐ The supplier (online or in-store) where I purchased my device (JB Hi-Fi, Bing Lee, OfficeWorks, etc.)
- ☐ Online sources (forums / blogs /podcasts / websites / online articles)
- ☐ Television, magazines, newspapers, radio
- ☐ The company that made my device (Apple, Hewlett Packard, Samsung, Dell, etc.)
- ☐ eSafety Commissioner
- ☐ Stay Smart Online
- ☐ ScamWatch
- ☐ Police
- ☐ Other government agency, not mentioned above
- ☐ Other

What was the **main** reason you reported the incident?

- I wanted the incident to be investigated by the authorities
- I wanted the perpetrators to be punished
- To warn others about the incident
- For insurance purposes
- To back get my money
- To get back my photos / files / non-monetary items, etc
- Other :Please specify_____

What was the **main** reason you did **not** report the incident?

- I didn't think reporting would result in any action or change
- I didn't think the incident was severe enough to warrant a report
- I didn't want anyone to know about the incident
- I didn't know I could report a cyber incident
- I didn't know who to report to
- I didn't find out about the incident for a long time and thought it was too late
- Other

-- Experimental section

- participants randomly assigned to see different advice on passwords and updating software -

When prompted on a personal device, how likely are you to update the software on the same day you were notified?

- Extremely likely
- Very likely
- Moderately likely
- Somewhat likely
- Not at all likely

How often do you leave the front door of your home unlocked?

- Always
- Sometimes
- Rarely / never

How often do you use a security alarm system in your home?

- I don't have one
- Always
- Sometimes
- Rarely / never

How often do you keep your valuables (such as a wallet, phone, or purse) in your line of sight when you are in public?

- Always
- Sometimes
- Rarely / never

How strong are these passwords?

	Very strong	Strong	Weak	Very weak
password1				
fieldhayfaretoss				
wjh63m&92mk11gr9				

How likely are you to create **strong** passwords for all of your important accounts?

- Extremely likely
- Very likely
- Moderately likely
- Somewhat likely
- Not at all likely

How likely are you to create **different** passwords for all of your important accounts?

- Extremely likely
- Very likely
- Moderately likely
- Somewhat likely
- Not at all likely

--end experimental section

Please indicate how much you agree or disagree with each of the following statements about digital security.

	Strongly agree	Agree	Partly agree / Partly disagree	Disagree	Strongly disagree
It is important to reduce the chance of cybercrime happening to me	☐	☐	☐	☐	☐
I could be a victim of cybercrime	☐	☐	☐	☐	☐
It is important to protect my personal details online	☐	☐	☐	☐	☐
I can take actions to reduce the chance of cybercrime happening to me	☐	☐	☐	☐	☐
My friends and family could be the victims of cybercrime	☐	☐	☐	☐	☐

	Strongly agree	Agree	Partly agree / Partly disagree	Disagree	Strongly disagree
I would NOT know if my computer, tablet or mobile phone's security was compromised	☐	☐	☐	☐	☐
I think it is up to individuals to protect their own privacy	☐	☐	☐	☐	☐
I am confident that organisations I use or I'm a customer of have security safeguards to protect my personal data	☐	☐	☐	☐	☐
It is important to protect the data of my customers / clients / suppliers from online security threats	☐	☐	☐	☐	☐

How much could you improve the digital security in your personal life?

- ☐ A lot
- ☐ A fair bit
- ☐ A little bit
- ☐ Not at all - I am completely secure

What stops you from improving your digital security?

Select all that apply

- ☐ Nothing
- ☐ I find the advice to difficult to follow
- ☐ I don’t have the time
- ☐ I think it costs too much
- ☐ I don't know where to go to find advice/information
- ☐ I don't think I need to improve my digital security
- ☐ I don't think my digital security is a priority
- ☐ I don’t think it will make any difference
- ☐ I already do all of the recommended things
- ☐ I don't think I have anything worth stealing

What is your **main** reason for having good digital security?

Select one answer only

- ☐ None - I don't think it's important to have good digital security
- ☐ To protect my money / assets
- ☐ To protect my personal documents including photos
- ☐ To protect my family
- ☐ To project my identity

- ☐ To reduce the chance of being embarrassed or shamed by others
- ☐ To reduce the chance of being blackmailed or compromised by others
- ☐ To reduce my chance of being bullied by others
- ☐ To reduce the time and financial costs of something going wrong
- ☐ Other :Please specify_____

Which one of the following best describes the industry or sector where you had a job last week?

If you had more than one job, select the option where you worked the most. If you are not sure, take an educated guess.

- ☐ Agriculture, Forestry and Fishing
- ☐ Mining
- ☐ Manufacturing
- ☐ Electricity, Gas, Water and Waste Services
- ☐ Construction
- ☐ Wholesale Trade
- ☐ Retail Trade
- ☐ Accommodation and Food Services
- ☐ Transport, Postal and Warehousing
- ☐ Information Media and Telecommunications
- ☐ Financial and Insurance Services
- ☐ Rental, Hiring and Real Estate Services
- ☐ Professional, Scientific and Technical Services
- ☐ Administrative and Support Services
- ☐ Public Administration and Safety
- ☐ Education and Training
- ☐ Health Care and Social Assistance
- ☐ Arts and Recreation Services
- ☐ Other Services

Who is responsible for day to day management of the IT security for your workplace?

Your workplace is where you worked the most last week

Select all that apply

- ☐ Me
- ☐ Another employee
- ☐ An IT specialist who is an employee of the business dedicated to IT
- ☐ Outsourced to an IT firm or contractor
- ☐ Family or friend
- ☐ Other
- ☐ Don't know

How would you compare your information security practices at work and in your personal life?

- ☐ Much better at work than personal

- Somewhat better at work than personal
- The same at work and personal
- Somewhat worse at work than personal
- Much worse at work than personal

Why do you think IT security is **better at work** than in your personal life?
If you had more than one job, think of the workplace where you worked the most last week
Select all that apply

- Because the organisation has people who look after IT and information security
- The organisation is concerned about protecting its data
- The organisation is concerned about protecting its reputation
- The organisation is concerned about customer, client or supplier data
- My work organisation is more likely to be targeted than me personally
- Other

Why do you think IT security is **better in your personal life** than at work?
If you had more than one job, think of the workplace where you worked the most last week
Select all that apply

- I use a service or software to help me with my personal digital security
- I am concerned with my personal data
- I am concerned about protecting my personal reputation
- I am concerned about protecting my children's, family's, or household's data
- Other

Finally we have a few questions about you. Your answers will not be used to identify you, but rather to analyse groups of respondents.

Do you have dependent children who live with you?
Yes
No

How old are the dependent children who live with you? *Select all categories that apply*
0-4
5-9
10-14
15-19
20+

What is your age group?
18 to 24
25 to 34
35 to 44
45 to 54
55 to 64

65 to 74
75 or older

Do you identify as Aboriginal and/or Torres Strait Islander?
Yes
No

Do you identify as someone living with disability?
Yes
No
Prefer not to answer

Is English your first language?
Yes
No
Prefer not to answer

Do you speak a language other than English at home?
Yes
No
Prefer not to answer

What is your gender?
Female
Male
X / indeterminate
Prefer not to answer

What is the postcode where you usually live? [_____]

Follow-up survey questions: cyber security survey of individuals

Three weeks ago, you participated in a survey that included information and advice about passwords. Do you remember reading about passwords in that survey?

- ☐ Yes
- ☐ No

In the last three weeks, did you create strong passwords across your important accounts?

Examples of important online accounts include, but are not limited to:
- Your online banking
- Your main email accounts
- Your social media accounts

- ☐ Yes for ALL of my important accounts
- ☐ Yes for SOME of my important accounts
- ☐ No

In the last three weeks, did you create different passwords across your important accounts?

Examples of important online accounts include, but are not limited to:
- Your online banking
- Your main email accounts
- Your social media accounts

- ☐ Yes for ALL of my important accounts
- ☐ Yes for SOME of my important accounts
- ☐ No

Is the following a strong password? *Horsecupstarshoe*

- ☐ Yes
- ☐ No
- ☐ Don’t know/unsure

Do you recall seeing information and advice in the survey three weeks ago about software updates?

- ☐ Yes
- ☐ No

In the last three weeks, have you received a notification to update your software or your computer, laptop, tablet or mobile phone?

- ☐ Yes
- ☐ No
- ☐ Not sure

How long after you got the update notification did you do the update?
If you got more than one update, think of the last one you received.

- ☐ Immediately (within a few hours)
- ☐ Within 1 or 2 days
- ☐ Within 3 to 7 days
- ☐ More than 7 days later
- ☐ Haven't done the update yet

When software needs to be updated, does it matter how soon you do so? *Select the best answer:*

- ☐ No, as long as you update eventually
- ☐ No, as long as you update within a week
- ☐ Yes, you need to update it within 24 hours
- ☐ Yes, the longer you wait the more vulnerable you are

Intervention advice

Advice used in the intervention for the survey experiment for individuals.

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!

Figure 11: Treatment cell A1: password security, financial consequences, no messenger

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!

Karl Hanmore
Acting Head
Australian Cyber Security Centre

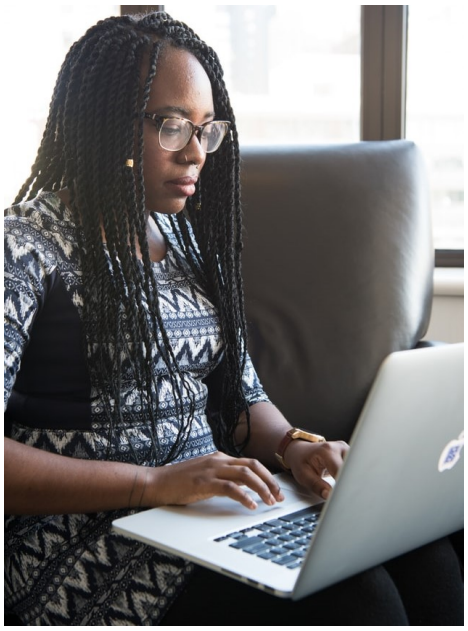
Figure 12: Treatment cell A2: password security, financial consequences, expert messenger

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!



Christina

Graphic Designer, Melbourne

Figure 13: Treatment cell A3: password security, financial consequences, peer messenger

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

How much are your files worth to you? Last year, 7,810 Australians reported being victims of hacking. Hackers regularly get access both directly and indirectly to important 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. You could lose photographs, personal details, or other online valuables, and sorting it out could take days or weeks of your time.

Protect your whole self online! 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!

Figure 14: Treatment cell A4: password security, non-financial conseqences, no messenger

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. How much are your files worth to you? Last year, 7,810 Australians reported being victims of hacking. You could lose photographs, personal details, or other online valuables; and sorting it out could take days or weeks of your time."

Karl Hanmore
Acting Head
Australian Cyber Security Centre

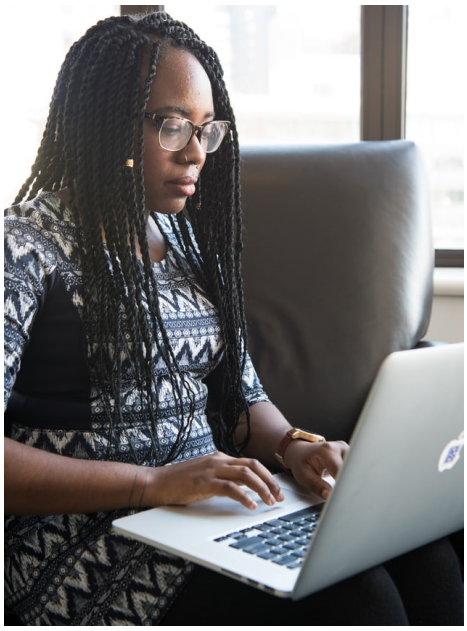
Here's Karl's advice for protecting yourself online:

- 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!

Figure 15: Treatment cell A5: password security, non-financial conseqences, expert messenger

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 locked me out of everything. I lost a few years' worth of important documents and photos and spent hours on the phone with IT specialists trying to resolve things."



Christina

Graphic Designer, Melbourne

Last year, 7,810 Australians reported being victims of hacking.

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!

Figure 16: Treatment cell A6: password security, non-financial conseqences, peer messenger

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.

Figure 17: Treatment cell B1: software updates, financial conseqences, no messenger

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.

"Programs and apps can have flaws in their security that only get fixed when you update the software. Older software like Microsoft Windows 7 is especially vulnerable. 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. Update your software before that point."

Are your devices updated? Last year in Australia, victims of malware and ransomware reported losing an average of almost $3,000.

Scott's advice for making 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 overnight or at a more convenient time.

Scott MacLeod

First Assistant Director-General
Protect, Assure and Enable

Australian Cyber Security Centre

Figure 18: Treatment cell B2: software updates, financial conseqences, expert messenger

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.

"Update your software. I clicked on a dodgy link in a text message, and because my phone wasn't up to date, it got infected with malware. They got into my bank account and I lost $10,800."

Annalise*
Teacher, New South Wales

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.

Learn from Annalise. 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.

Figure 19: Treatment cell B3: software updates, financial conseqences, peer messenger

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.

Figure 20: Treatment cell B4: software updates, non-financial conseqences, no messenger

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.

"Programs and apps can have flaws in their security that only get fixed when you update the software. Older software like Microsoft Windows 7 is especially vulnerable. 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. Update your software before that point."

Are your devices updated? Last year in Australia, 4,359 people reported being victims of malware or ransomware.

Scott's advice for making 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 overnight or at a more convenient time.

Scott MacLeod

First Assistant Director-General

Protect, Assure and Enable

Australian Cyber Security Centre

Figure 21: Treatment cell B5: software updates, non-financial conseqences, expert messenger

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.

"Update your software. I clicked on a dodgy link in a text message, and because my phone wasn't up to date, it got infected with malware. It locked me out and I lost years' worth of photos and files."

Annalise*
Teacher, New South Wales

Last year in Australia, 4,359 people reported being victims of malware or ransomware. 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.

Learn from Annalise. 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.

Figure 22: Treatment cell B6: software updates, non-financial conseqences, peer messenger

Sources

Outcome	Consequence	Messenger	Source
Passwords	Financial	Attention Control	From Hacking (Scamwatch, 2019) 7,810 reports with 6% financial losses = 467 financial victims losing $4,543,740; avg of $9,729.63.
		Peer Messenger	
		Expert Messenger	
	Non Financial	Attention Control	From Hacking (Scamwatch, 2019). 7,810 reports
		Peer Messenger	From Hacking (Scamwatch, 2019). 7,810 reports. Case Study provided by 24/7 Global Watch: A 32 year old woman repeatedly lost administrator rights on her personal laptop over a number of months. In addition to the issues with the personal laptop, the victim's internet service was remotely accessed by an anonymous user, and an unknown application was found to have been installed on her mobile telephone. As a result, the victim required specialist IT service providers attend her home **on more than seven occasions**, resulting in the repeated loss of documents and personal data.
		Expert Messenger	From Hacking (Scamwatch, 2019). 7,810 reports
Updates	Financial	Attention Control	From Malware & ransomware (Scamwatch, 2019) 4,359 reports with 1.2% financial losses =52.3 financial victims losing $155,669; avg of $2,993.64
		Peer Messenger	Case Study provided by 24/7 Global Watch:

Outcome	Consequence	Messenger	Source
			A 56 year old man received an **SMS text message** from what he thought was his financial institution, which stated they had detected a potential issue with his account and had 'blocked' it. The message directed the man to click a **malicious link** to have his account 'unblocked'. The victim clicked the link, leading him to a malicious website which prompted him to login using his online banking credentials. The victim was further prompted to provide his driver's license number and mobile phone number. The victim believed this would unblock his account, when in fact he had given malicious actors his personally identifiable information. **The victim lost a total of $10,800 after a malicious actor transferred funds out of his bank account.**
		Expert Messenger	From Malware & ransomware (Scamwatch, 2019) (as in Att'n Control)
	Non Financial	Attention Control	From Malware & ransomware (Scamwatch, 2019). 4,359 reports.
		Peer Messenger	From Malware & ransomware (Scamwatch, 2019). 4,359 reports.
		Expert Messenger	From Malware & ransomware (Scamwatch, 2019). 4,359 reports.

References

Hadlington, L, Parsons, K, Calic, D & Butavicius, M (2019). 'Beyond the workplace: Exploring Information Security Awareness and the role of impulsivity and cognitive failures' Manuscript submitted for publication.

Lakens, D (2016) 'Why you don't need to adjust your alpha level for all tests you'll do in your lifetime' Blog post, 14 February, https://daniellakens.blogspot.com/2016/02/why-you-dont-need-to-adjust-you-alpha.html

Muralidharan, Romero and Wuthrich (2020) 'Factorial designs, model selection, and (incorrect) inference in randomized experiments' Working Paper (5 February) https://econweb.ucsd.edu/~kamurali/papers/Working%20Papers/CrossCuts%20(Current%20WP).pdf

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 www.pmc.gov.au/beta