Pre-analysis plan: Engaging small business in cyber safe practice.

While we did not publicly pre-register this trial prior to data collection, we did pre-register this pre-analysis plan before commencing analysis of this trial. This occurred on 29 October 2019.

Policy problem and trial aims

Policy problem

Small and medium enterprises are at risk of ransomware attacks and phishing attacks on their business IT systems.

Businesses can protect themselves by downloading software updates as soon as they become available, by regularly backing up their data and by avoiding clicking on links to unfamiliar URLs in emails.

Many small and medium enterprises are unaware of these simple steps that could help protect their business. The Australian Cyber Security Centre (ACSC) provides advice for small businesses. It publishes this on its website www.cyber.gov.au and is interested in how best to present this information and advice so that it is maximally effective in improving awareness and behavioural change.

Trial aims

The trial aimed to test advice on phishing, downloading updates and backing up data. We tested presenting this advice in different formats: including plain text, infographics and an interactive quiz with infographic.

Trial design, sampling and population

This was an individually randomised survey experiment delivered as part of a survey collecting information on the cybersecurity behaviours of small and medium

enterprises (SMEs). The survey and experiment were collected through an online survey platform (Qualtrics).

The initial survey took roughly 9 minutes to complete. Randomisation into one of four groups, and then exposure to the intervention occurred after the main body of survey questions were complete. Individuals then completed a second short survey to gather outcome data. All groups responded to the same set of outcome measures and were invited to participate in the follow-up survey. The follow-up survey was identical for all treatment groups.

The initial experimental design was piloted on a sample of 461 individuals and interventions were refined based on this pilot.

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). 1553 individuals commenced the survey with 1186 individuals randomised into the experiment.

Interventions

C. Control – Respondents proceed directly to the outcome survey without exposure to information/advice.

T1. Plain text – Respondents read three short pieces of information/advice about detecting phishing emails, software updates and backing up data.

T2. Infographic – Same information/advice as above, but presented as an infographic.

T3. Interactive infographic – Quiz style question on each topic, followed by the previous infographic explaining the correct answer.

Outcome measures

Primary outcome measures:

There are three *primary outcomes* for this trial. Outcome 1 is based on the response to a test and Outcome 2 & 3 are self-reported.

Outcome 1 - Phishing test score

Individuals completed a phishing test, where respondents are presented with three emails and decide if they are genuine or fake. The order of emails was randomised. One email was genuine and two were fake.

Outcome measurement: Average number of correct answers.

Outcome 2 and 3 - Self reported outcomes

Individuals were asked about their intentions to update their software and intention to backup their data. Questions 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 back-ups of business data?’

For both of these outcomes, response options were identical:

1. System is already in place
2. Definitely
3. Likely
4. Unlikely
5. Definitely not

Outcome measurement: A binary variable will be derived in which: ‘System is already in place/Definitely’ = 1 and ‘Likely/Unlikely/Definitely not’ = 0.

For our self-reported outcomes, we will also perform a secondary analysis in which we treat the survey scale as continuous (but collapsing ‘System already in place’ and ‘Definitely’ together). We will use this to aid the interpretation of our primary outcomes.

Secondary outcome measures:

Those who participated in the RCT and completed the post intervention survey were offered the opportunity to be contacted after 3 weeks for a follow-up survey.

In the follow-up survey, we asked a number of questions relating to phishing, update and backup behaviours. We will compare prevalence of these behaviours across groups to look for evidence of behaviour change (as opposed to changes in intention, measured in our primary analysis). Due to the small number of participants opting for follow-up, we do not think these results will be robust.

Hypotheses

H1: Behavioural intentions and phishing identification will be higher among respondents exposed to any treatment compared to control (T1-3 pooled > C).

H2: Behavioural intentions and phishing identification will be higher among each of our treatment groups compared to control (T1-3 > C).

H3: Behavioural intentions and phishing identification will be different between respondents who receive cyber security advice as an infographic vs text (T2 ≠ T1).

H4: Behavioural intentions and phishing identification will be different between respondents who receive cyber security advice as an interactive infographic vs text (T3 ≠ T1).

H5: Behavioural intentions and phishing identification will be different between respondents who receive cyber security advice as an infographic vs an interactive infographic (T3 ≠ T2).

Sample size and power calculations

We had a final sample of 1186, which gave us approximately 300 individuals per group. When we ran our power calculations, we used a fixed sample size of 250 individuals per group. Baseline prevalence levels for our outcomes were taken from the control group outcomes in our pilot RCT.

The trial has power to detect a minimum effect size of 0.25 (Cohen's h) on the **phishing test** assuming 80% power and a 5% significance level (Figure 1).

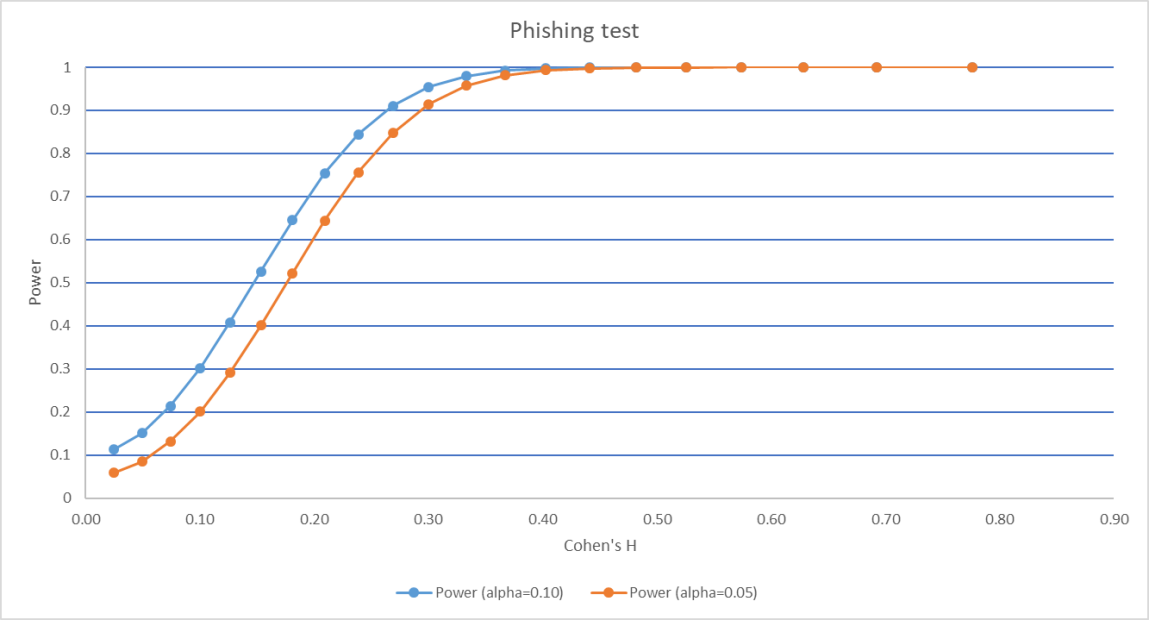

Figure 1: Power curve for phishing test

The trial has power to detect a minimum effect of 10.5 percentage points on the **updates intention** assuming 80% power and 5% significance level

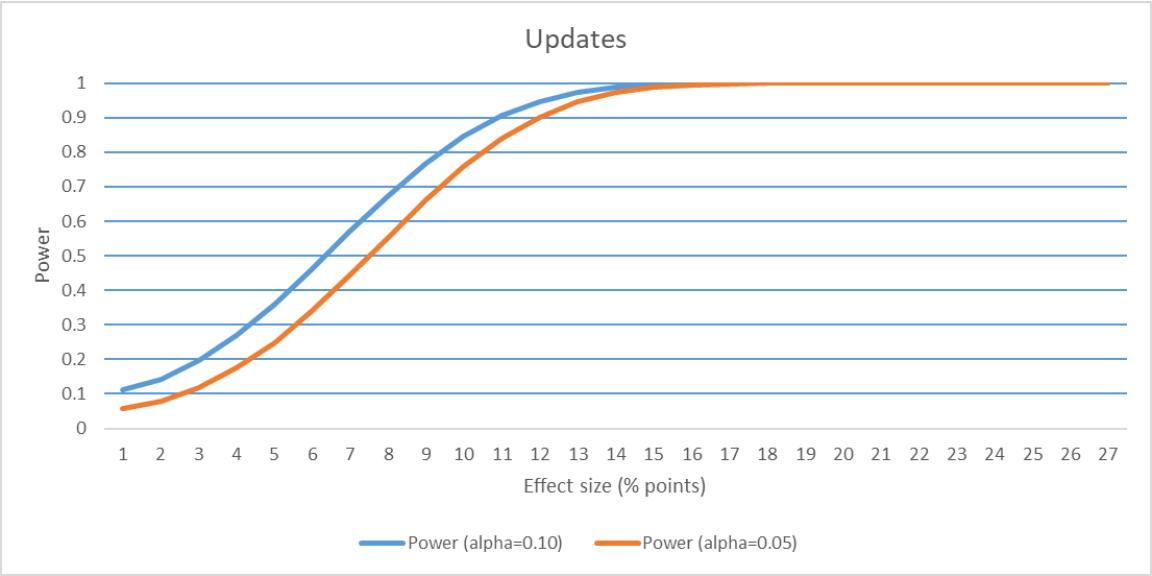

Figure 2: Power curve for intention to update software

The trial has power to detect a minimum effect size of 8.6 percentage points on the **backups intention** assuming 80% power and 5% significance level (Figure 3).

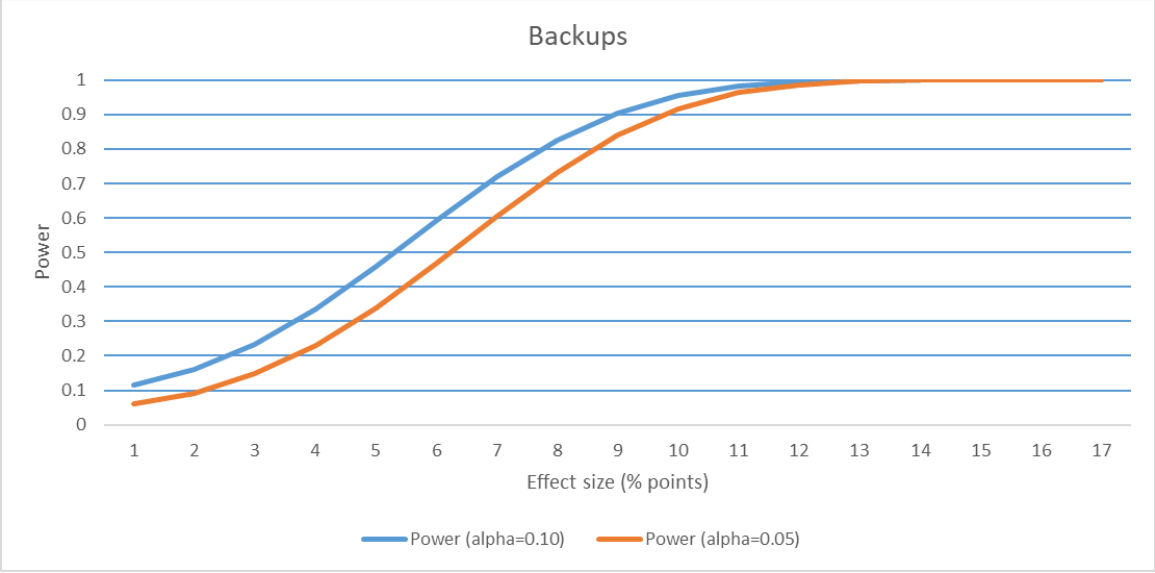

Figure 3: Power curve for intention to back up

Method of analysis

The principal analysis of the effect of the intervention will be an adjusted comparison of our primary outcomes. These estimates, confidence intervals (CI) and p-values will be derived from a linear regression model with the following specification:

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

Where y is one of our three primary outcomes (see Outcome Measures above), 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 (as per Lin (2013)), and ε is an error term which picks up variance not explainable by treatment indicators or covariates.

Exact p-values and confidence intervals will be reported. Our primary analysis will not adjust for multiple comparisons. However, we will exercise caution interpreting the results of the primary analysis in light of the number of comparisons. To aid with interpretation we will report Bonferroni corrected p-values in the technical appendix (noting that adjusted p-values will be conservative due to the assumption that all tests are independent and belong to the same family).

Covariates

We conducted a baseline survey prior to randomisation, covariates were selected based on a series of regressions on the pilot dataset.

Table 1. 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 (Phishing test)
Past behaviour - downloading software updates	Self-rated “automatically or frequently updates software”	Binary	Outcome 2 (updates)
Past behaviour - backing up data	Self-rated “automatically or frequently backs-up data”	Binary	Outcome 3 (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

Covariate Description	Derived from	Type	Included for outcome
Device type	desktop vs mobile device from Qualtrics metadata	Binary	All

Device type (recorded by Qualtrics) is included, as the interventions and phishing test look slightly different on a mobile device compared to a larger screen. The Phishing test also lacked the capability to 'hover' the cursor over URLs when viewed on a mobile device, so the URLs were inserted statically.

Missing data

- We expect 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 are no forced responses). Although this is unlikely to be related to treatment status, we will examine our data for evidence of differential attrition.
- Survey respondents who were randomised but did not provide a response for a given outcome will be excluded from the analysis for that outcome (but will be included for other outcomes if they provided a response).
- We will include missingness dummies to account for missing covariate data.
- Non-response bias is expected to be an issue as the kinds of businesses who respond to a non-compulsory online survey, may be different in many ways to those who do complete. This creates an issue around generalisability, which we will take into account in our discussion of results.

Pre-analysis plan commitments

- No analysis has been undertaken prior to the completion of this pre-analysis plan.
- We will be transparent about, and provide justification for, any deviations (additions or omissions) from this plan.
- We will include the survey questions in the published report