DESIGNING PHISHING SIMULATIONS

A QUICK REFERENCE GUIDE FOR ORGANISATIONS

Don't take the bait

National Protective Security Authority

UNIVERSITY OF BATH

DISCLAIMER

OVERVIEW

Phishing simulations within organisations provide a way to better understand potential vulnerabilities of employees to phishing emails. In order to get the most out of simulation exercises, a structured and systematic approach should be used that will allow findings to be compared over time and across groups.

This quick reference guide provides a starting point for designing phishing simulations according to a desired end-point and the particular questions that you are interested in understanding. This includes:

- Identifying key questions that you would like to answer

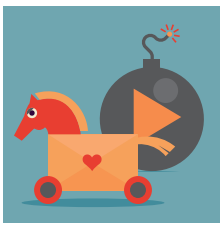
- Designing systematic simulations that enable these questions to be addressed

1.
IDENTIFYING KEY QUESTIONS THAT YOU WOULD LIKE TO ANSWER

When designing a phishing simulation, it is important to first consider what it is you want to know and how the data will be used. This will drive all elements of the design of your simulation. For example:

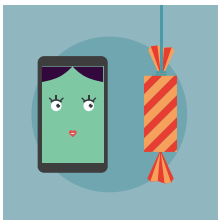
Are some groups of employees more susceptible to phishing emails than others?

If you are interested in knowing the answer to this you could divide personnel into groups according to their length of time in the organisation, their job role, their clearance level, or their location and then comparing response rates across these groups. This may be used to develop targeted initiatives for particular employee groups.



Has employee susceptibility to phishing emails changed over time?

If you are interested in knowing the answer to this you could undertake a simulation at a set point in time, undertake a second comparable simulation at a later date and then compare response rates across the two time points. This may be used to assess the impact of an intervention, such as the roll-out of new training between these time points.



Are employees more susceptible to certain types of threat?

If you are interested in knowing whether employees are more susceptible to particular types of phishing emails then you can compare responses to different types of phishing simulations. This may relate to the types of phishing emails that employees typically receive and will help identify particular vulnerabilities that your organisation may have. For example, internal versus external emails, or those which use different techniques (e.g. claiming to offer a reward versus a potential loss of access to an account). This can then be used to prioritise training and awareness campaigns in relation to these types of attack.

Having decided on the key questions that you would like to answer, you can then move on to the design of a systematic simulation that addresses these.

2.
DESIGNING SYSTEMATIC SIMULATIONS

Once the key questions of interest have been determined, the best method to answer them using a phishing simulation can be identified. The questions will determine how many simulation emails are likely to be used, how different or similar these emails should be, and the sample size that is likely to be required.

For all your questions of interest, it will be important to consider the following:

How many people you are able to test

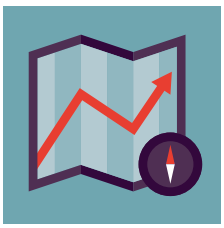
(your sample size)

How often you are able to run phishing simulations

(simulation frequency)

The geographic distribution of your sample

(are recipients based in one location or distributed across multiple locations?)



What your measures of success will be

These may include:

- o How many people click on a link (the click-rate)
- o How many people enter user credentials when prompted (the disclosure rate)
- o How many people report the email (the reporting rate)

All of these aspects may impact on both the design of the simulation and the resources required to manage it.

Example questions and methods for testing three question types are provided on the next few pages.

EXAMPLE QUESTION A:
Are newly recruited personnel more or less susceptible to phishing emails?

QUESTION TYPE:
Exploring response differences across groups

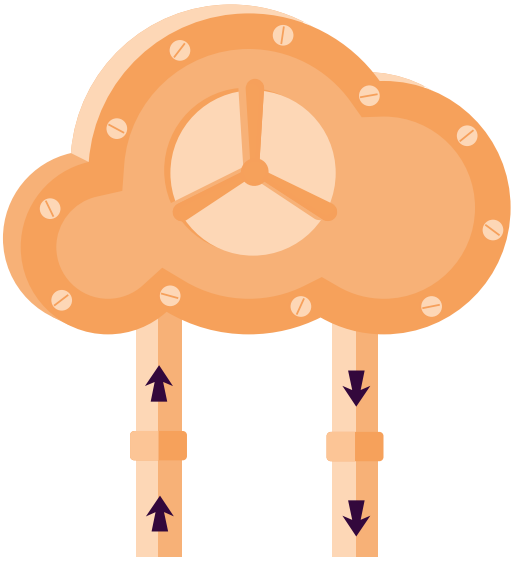
Once you have chosen a group category (e.g. length of time in organisation), you can determine who will be included in each group (e.g. under 1 year, 1-4 years, 5 years or more). An equal number of people should be included in each group. The groups should be similar in all other aspects apart from your factor of interest (e.g. similar gender proportions, similar degree of training, similar job role proportions etc.). This is to ensure that any differences between the groups are due to your factor of interest and not something else.

If possible, the same email should be sent to all groups. If this is not possible, then the emails should be as similar as possible (e.g. similar content, length, layout, use of images, sender address). Emails should also be sent to all of the groups over the same period of time. This is to make sure that any response differences are not due to other differences in the simulation exercise.

Groups to consider when designing phishing simulations:

- Length of service
- Seniority e.g. grade if civil service, ranks, management, senior management
- Location of office e.g. UK based or overseas branch
- Department e.g. sales, R+D, finance

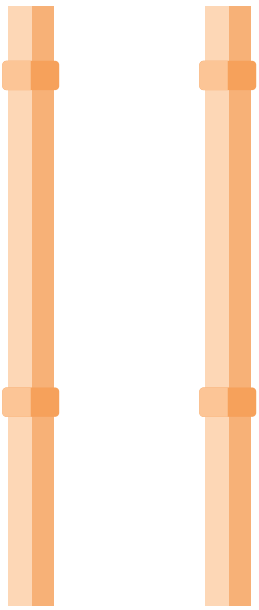
EXAMPLE QUESTION B: Has your recent awareness campaign on phishing emails had an impact?



QUESTION TYPE: Exploring response differences over time

If you have decided to focus on response differences over time, then you do not need to divide employees into separate groups (unless you are combining both group differences and changes over time). You may decide to compare responses before or after an intervention, or responses at different times of the week (e.g. Monday morning versus Friday afternoon).

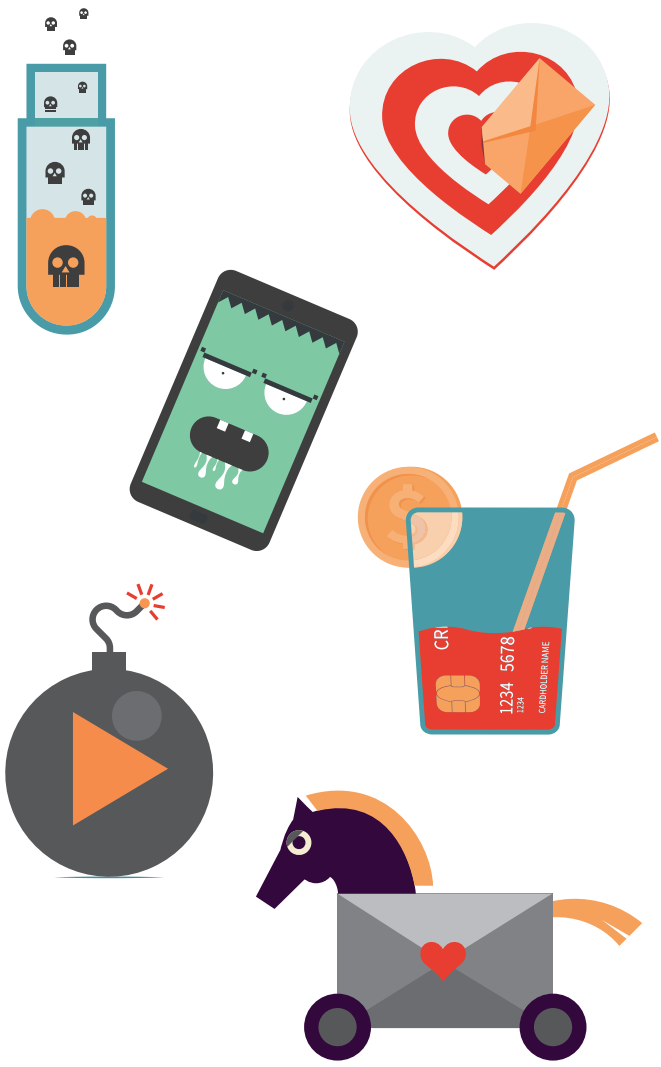
Ideally, this design involves sending emails that are as similar as possible to the same group of employees (e.g. the same people receive both simulation emails) at two different time points. However, if this is not possible, then employees who receive the email at time point 1 should be as similar as possible to those who receive the email at time point 2 (e.g. similar gender proportions, similar degree of training, similar job roles etc.). This is to reduce the chance that any response differences are due to contrasts in either the simulation email received or employee differences.



EXAMPLE QUESTION C: What type of phishing email is your organisation most vulnerable to?

QUESTION TYPE: Exploring response differences across email types

If you have chosen to focus on response differences across email types, then as above, differences in employees who receive the email and differences in when the email is received should be minimised as much as possible. The only difference should be the chosen aspect of the email itself. Ideally, only one email aspect should be changed (e.g. an email contains a logo versus not, or using an external versus internal looking email address). Each type of email can then either be sent to the same employees or different employees (if they have been matched for similarity).



Finally, some additional tips to consider when designing your simulation:

Keep it simple and don't try to answer too many questions at once. The general rule is the more questions that you try to answer, the larger the sample that you will need.

Use the largest sample size possible. In general, the more people who can be sent the simulation, the more robust your findings will be.

Don't try to do too much at once. Prioritise your questions of interest and keep it simple.

Highlight the personal relevance of exercises to employees. Vulnerability in the workplace may be reflected in vulnerability at home.

Provide learning and advice at the time of 'clicking'. This may be in the form of redirection to advice pages or online training modules.

Avoid sending the same simulation email to too many people working in close proximity, as responses are likely to be driven by how many others received the same email.

National Protective
Security Authority

UNIVERSITY OF
BATH