Assessing the Perceptions of Phishing Awareness Campaigns: A Methodology for Customised Delivery to Improve Training Outcomes

[redacted]
Faculty of Design, Informatics and Business
Abertay University
DUNDEE, DD1 1HG, UK

ABSTRACT

Context
Phishing campaigns continue to provide the single largest entry point for successful cyber-attacks. Simulated phishing campaigns are currently used to improve the awareness of employees. Generic and impersonal simulation content can impact the success of training campaigns.

Aim
To investigate the perceptions of phishing training campaigns on their participants, and how that impacts on desired outcomes. An adaptive methodology will be implemented with the goal of improving the effectiveness of such campaigns.

Method
A methodology for delivering customised training content will be developed, supported by a proof-of-concept phishing simulation platform (PhishSim). The platform will have the functionality to send follow-up user questionnaires to users, the results of which will be used to inform the content of successive awareness campaigns. Customised content will be developed using responses received from subjects who have experience in participating in phishing awareness campaigns.

Anticipated Results
Phishing training content that can be tailored, informed by user responses to a generic template, can increase user awareness, improving training campaign outcomes.

Keywords
Phishing awareness, Human factors in cyber security, Cybersecurity training, Awareness programs, Security culture, Customised training

1. INTRODUCTION
According to the Department for Science, Innovation & Technology (DSIT), 84% of successful cyber-attacks were attributable to phishing emails (2024), making it the most common attack vector across the organisations surveyed. Figure 1 shows the top five attack methods identified, demonstrating the dominance of phishing as an entry point for cyber-attacks. The implications for an organisation falling victim to a successful cyber-attack can be both multifaceted and highly impactful - a successful phishing attack carried out on the Scottish Environment Protection Agency (SEPA) in 2020 continues to cause reputational damage following a ransomware infection initiated by a phishing email (Futurescot, 2022).
Furthermore, phishing attacks were identified as the most disruptive attack vector for an organisation in DSIT's (2024) report, with 61% of businesses reporting this finding. The average cost of the most disruptive attack for medium/large organisations was £10830 (DSIT, 2024), demonstrating significant financial losses for those affected. Figure 2 shows the comparative figures for costs across other organisation categories covered in the report.

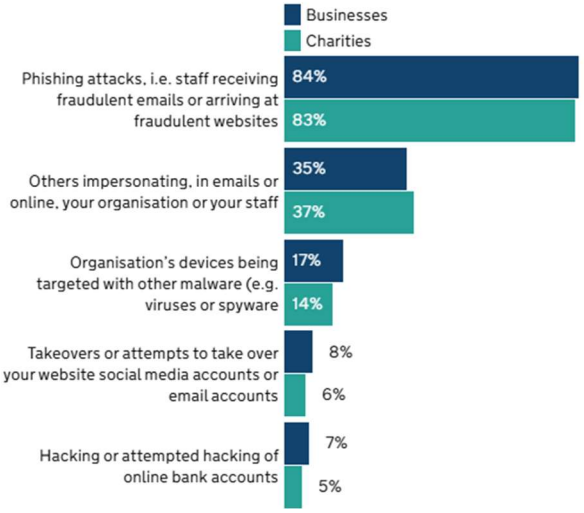

Figure 1: Percentage of types of breaches or attacks among the organisations that have identified any breaches or attacks (DSIT, 2024)

Across organisations identifying any breaches or attacks	All businesses	Micro/small businesses	Medium/large businesses	All charities
Mean cost	£1,205	£780	£10,830	£460
Median cost	£0	£0	£50	£0
Base	1006	740	266	424

Figure 2: Average total cost of the most disruptive breach or attack (DSIT, 2024)

Phishing email objects themselves pose no threat without active user interaction. The techniques used to initiate a cyber-attack in phishing emails can be broken down into categories. Proofpoint (2024) use the following categorisations in its "State of the Phish" report:

- Link-based.
- Data entry.
- Attachment.

These categories are outlined broadly in Table 1.

These techniques have given rise to some common guidance given to users on how to identify a malicious email, such as the advice to hover the mouse cursor over links embedded in e-mails so that the address can be scrutinised before clicking on them. Users in this instance need to have the skills to

identify not only if the URL is genuine, but also to identify intentionally misleading spelling mistakes (e.g. off1ce.com instead of office.com). Historically this advice about spelling mistakes extended to the content of the email, though this is becoming a less reliable indicator with the rise of artificial intelligence (AI) that will automatically generate grammatically correct content when requested (Eze and Shamir, 2024). Advice from the NCSC (2025) also suggests that users should consider the familiarity of the sender and the tone of the email content as contributing factors towards whether they deem an e-mail to be genuine or not.

Table 1: Phishing technique category definitions

Technique type	Technique process
Link-based	The recipient clicks on a link in the phishing email, which directs them to a site that attempts to download malicious software to the user's computer.
Data entry	The recipient clicks on a link in the phishing email, which directs them to a site that prompts them to enter personal information, such as credentials or credit card information. This information would then be harvested by the attacker.
Attachment	The recipient opens an attachment in the phishing email, which hosts a script to install malicious software on the user's computer.

Proofpoint's (2024) report into phishing attacks suggests that 71% of users who received a suspicious email took a risky action. Of those users, 96% were aware that the actions they chose to take were risky. Consequently, 69% of the organisations surveyed were infected by ransomware as a direct result of user interaction with a malicious email. These figures indicate the need to ensure that users not only have the knowledge to identify phishing e-mails, but that they also understand the consequences that risky actions could have on their organisation. Proofpoint (2024) posits that security awareness training should be used as part of a program of work to address the lack of user knowledge, thereby reducing the risk posed by users. Their report further suggests that any such awareness campaigns should be agile to ensure that they remain relevant and effective (Proofpoint, 2024).

Research suggests that simulations are the most common method used to improve staff awareness of phishing emails (Althobaiti and Alsufyani, 2024). These exercises involve the sending of fake yet realistic phishing emails to employees with the intention of capturing the response of those employees to determine whether further training is required. Campaigns can be targeted at groups of individuals, to entire teams, departments, or the organisation as a whole. Typically, the contents of the fake emails, and the workflows associated with the actions taken by users, are the same across all participants of the exercise.

This project aims to examine to what extent phishing training campaigns could be adapted to address adverse effects on their participants. The implementation of a flexible and customisable methodology will be evaluated within a proof-of-concept environment to analyse how the framework could be adapted to the needs of end users and improve upon the desired outcomes for those campaigns.

2. BACKGROUND

It is widely accepted that organisations should implement security awareness programs to assist in the risk reduction of successful cyber-attacks against the business (Whitman and Mattord, 2019). Given the continued dominance of phishing campaigns as an attack vector for successful cyber-attacks, it can be argued that any awareness programs implemented should include an emphasis on training users on the appropriate behaviours to exercise when interacting with an e-mail they deem suspicious (Tschakert and Ngamsuriyaroj, 2021). Despite the widespread adoption of phishing simulation exercises to educate end-users about phishing emails and the consequences of interacting with suspicious communications (NCSC, 2024), organisations continue to experience disruptions caused by successful phishing campaigns.

2.1 Organisational culture

Schneier (2000) posits that, in the chain that represents security, people are the weakest link. He further credits people with being "chronically responsible for the failure of security systems" (Schneier, 2000, p.255). This mindset of blame, focused on the end-user, has perpetuated its way into organisations, despite research suggesting that this attitude is counter-productive to achieving the desired training outcomes for users (Renaud, Musarurwa and Zimmermann, 2021). Renaud et al further suggest that an organisational culture that targets and punishes individuals for failing to achieve an expected standard of cyber security awareness can have wide-reaching consequences on the cyber security posture of an entire staff. They argue that this treatment of employees can instil a counterculture of distrust and guilt, causing users to disengage with training programs entirely out of fear of failing to meet expectations (Renaud, Musarurwa and Zimmermann, 2021).

2.2 Phishing simulations

Educating users not to interact with suspicious messages is a complicated issue because the root issue does not target a vulnerability in a technical component but a psychological one (Jari, 2022). The contents of phishing emails are specifically crafted to appeal to an individual's human weaknesses. This introduces a delicate challenge about how these weaknesses can be patched, as would be the approach with technical vulnerabilities. Phishing simulations are the proposed (and largely implemented) solution to this problem, allowing an administrator to compose fake phishing emails that closely mimic those that would be seen in a genuine attack attempt. Should a user fail to identify a phishing email correctly, the standard approach is to offer that individual targeted training, though some reports suggest that some organisations implement formal disciplinary procedures for those that fail the test (Segal, 2022).

2.3 User perceptions of phishing simulations

There are differing reports on the opinions of employees regarding the use of phishing simulations as training awareness tools. Rizzoni et al (2022) found that these campaigns can instil a feeling of distrust in the targeted staff, leading them to believe that they were under scrutiny. The user feedback from this study suggested that participants would have been more receptive to the program if they had been aware it was being conducted and if the email content

had been tailored, rather than using the same content for all. Conversely, Schiller et al (2024) could not find any evidence to suggest that phishing simulations made participants feel as if they were being attacked. Furthermore, their findings suggest that the desired outcomes of the training program were sufficiently met, with employees implementing new and more vigilant methods for dealing with potentially suspicious emails. The authors of this study signpost a number of external studies that have posited the use of phishing simulation exercises as "controversial", in contradiction to their own findings. It should be noted that both studies have a limited testing base, using a single company as the sole source for all participants.

2.4 Effects of user perceptions

Jari (2022) highlighted the lack of customisable content for phishing emails as a contributor to poor outcomes from awareness programs. Targeted users were less likely to engage with the campaign in instances where they were unable to relate to the email content, thus failing to benefit from the training objectives of the campaign. A comparative literature review conducted by Jampen et al (2020) further supports the argument that the use of tailored content for phishing simulations would improve the success of training campaigns, though their suggestions for customised content centre around demographical characteristics, rather than user emotional response to those campaigns. This project aims to expand upon the findings of the research already conducted, analysing the responses of users from a varied field of participants of pre-existing phishing simulation exercises to determine the effect that their emotional responses can have on the success of phishing awareness campaigns

3. METHOD

The aim of this project is to create a methodology that can be implemented to deliver phishing awareness exercises with tailored content. A proof-of-concept phishing simulation platform (PhishSim) will be created to demonstrate the implementation of the methodology in a production environment.

3.1 Objectives

The finalised methodology should provide a framework for administrators on how to scope, plan, and implement their phishing awareness campaigns using a baseline exercise and follow-up user feedback questionnaires. Guidance will be provided on how to analyse the results of the user responses, with direction given on how to develop exercise content in response to the resulting analysis. Suggestions of potentially suitable exercise content variations will be included within the methodology documentation.

3.2 Methodology

A hybrid research approach (using qualitative and quantitative techniques against questionnaire responses) will be used to inform the construction of the methodology. The target audience will be any end-users who are, or have ever been, participants in corporately organised phishing simulation exercises intended to improve cyber security awareness. The questionnaire will be conducted on a fully anonymised basis. The questions posed will centre around two main themes:

1. Fact driven questions around when and how awareness campaigns were/are being implemented, with a particular emphasis on the consequences for "failing" users.
2. Open-ended questions around user perceptions of the awareness campaign they participate(d) in, with a particular focus on how they felt about the consequences of failing. Sample alternatives will be shown, with participants asked to evaluate how they would feel about receiving each in the event of a "failure".

The responses from the questionnaires will be used, along with findings from a literature review, to inform the creation of the methodology. It is envisaged that the methodology will consist of the following loose framework:

- Scoping/planning/implementing a baseline awareness campaign.
- Conducting user feedback reviews and analysing the results.
- Scoping/planning/implementing successive awareness campaigns.

In order to demonstrate the implementation of the methodology in a production environment, a proof-of-concept phishing simulation platform (hosted within a virtual environment) will be created.

3.3 Virtual environment set-up

Quasi-experimentation will take place within an isolated virtual environment hosted in Oracle VirtualBox. A Ubuntu Server instance will provide the following services in order to implement the methodology:

- Graphical user interface.
- Postfix SMTP mail server (to send campaign emails to users).
- Dovecot IMAP server (enables users to view campaign emails in a graphical interface).
- HTTP Apache server (to host a graphical interface for the platform management console).
- mySQL server (to host a database of users and groups for the platform).
- Python (scripting language for the management console interface).
- Flask (web framework for the management console interface).
- Splunk server (for ingestion and analysis of user feedback responses).

A small pool of test user accounts will be created using a fake name generator. At this stage of the research, these will not be "real" users - rather, the user objects will be used as a mechanism to explore how the system and methodology can be manipulated. It is anticipated that six accounts will likely cover an appropriate number of variations from user responses to demonstrate the methodology, but this can easily be increased.

3.4 Phishing simulation platform creation

The flow of the phishing simulation platform functionality will follow the loose process outlined in Figure 3. The platform will be accessed using a graphical web page front end operating on a LAMP (Linux/Apache/mySQL/Python) web application stack. The web application will use the Flask web framework functionality to connect to the Postfix SMTP server to send e-mails related to the phishing awareness campaign. Consideration (informed by the responses received from questionnaires completed by research participants) will be given to the design and semantics of the emails sent to users and to the feedback

questionnaires that can be sent to end-users following the completion of the campaign. Further Flask functionality will be utilised to connect to the mySQL database to source the user details (including email addresses) for the campaign. It is intended that the interaction between the web application and the database will allow the administrator to update the database from within the management console. Splunk will be configured to monitor a local directory for user responses to the feedback questionnaire, automatically ingesting them and thus provide the capability to quickly analyse the results both graphically and textually. Finally, the management platform will provide functionality to allow the administrator to customise and create content for both phishing simulation emails and user feedback questionnaires.

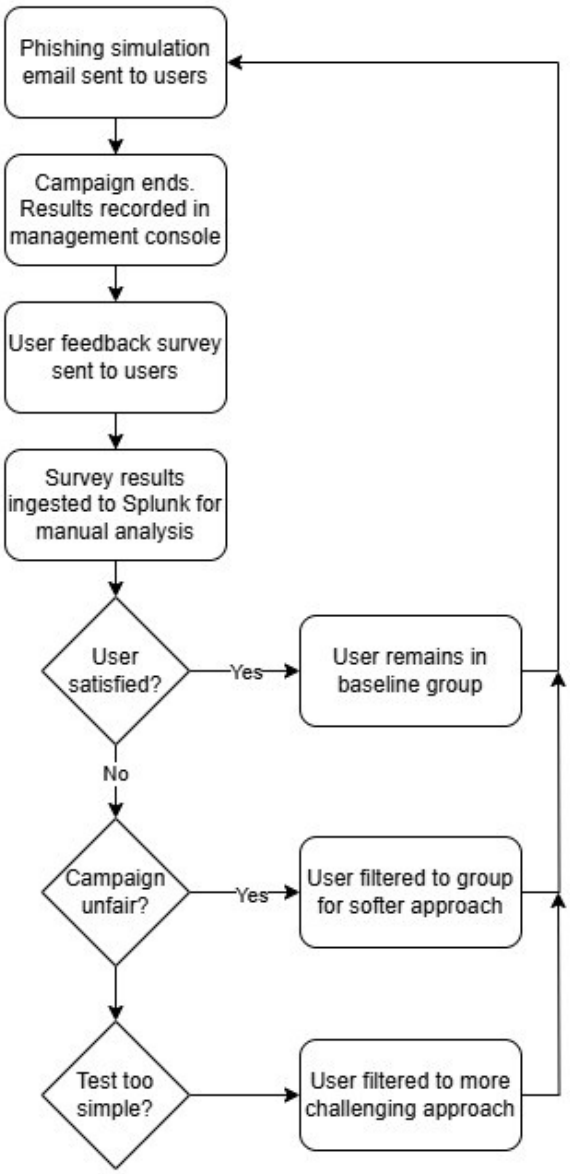

Figure 3: flowchart showing functionality of phishing simulation platform

3.5 Possible problems

Of particular concern is whether enough research participants can be recruited to complete the user questionnaires, and that the pool of participants is sufficiently varied so as to avoid sample bias. These responses are expected to inform the content for the phishing simulation emails and the feedback questionnaires which will form the basis for a critical part of the methodology. It may be possible to conduct further literature review to counter-act this. As a further mitigation, priority will be given to the development and distribution of the user questionnaires, allowing more time for the recruitment of participants and analysis of results.

4. CONCLUSION

This research project aims to analyse the effects of user perception of phishing awareness campaigns on the outcomes of those same campaigns. There will be a focus on how the actual outcomes compare with the intended outcomes. An evaluation of whether campaign outcome improvements could be achieved with the implementation of a methodology that allows for customisation of training content, tailored to the needs of groups of users will be conducted. A created methodology will offer a framework for implementation in a production environment, with flexibility for both users and administrators at its core. The practical implementation of the methodology will be exhibited with a proof-of-concept web application, thus demonstrating the ease with which it could be adopted into a production environment. It is anticipated that users offered the opportunity to participate in campaigns with personalised content would show both higher levels of engagement and improved learning outcomes. Furthermore, it is expected that this heightened level of awareness and improved behaviours when interacting with suspicious messages could not only assist in the prevention of successful cyber-attacks but also contribute to a more positive organisational culture with regards to cyber security.

5. REFERENCES

Althobaiti, K. and Alsufyani, N. (2024) 'A review of organization-oriented phishing research', *PeerJ Computer Science,* 10 Available at: https://doi.org/10.7717/peerj-cs.2487.

Beu, N., Jayatilaka, A., Zahedi, M., Babar, M.A., Hartley, L., Lewinsmith, W. and Baetu, I. (2023) 'Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation', *Computers & Security,* 131 Available at: https://doi.org/10.1016/j.cose.2023.103313.

Department for Science, Information & Technology. (2024) *Cyber security breaches survey 2024.* Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 (Accessed: 2 March 2025).

Eze, C.S. and Shamir, L. (2024) 'Analysis and Prevention of AI-Based Phishing Email Attacks', *Electronics,* 13(10) Available at: https://doi.org/10.3390/electronics13101839.

Futurescot (2022) *'Human error' caused by phishing email likely source of SEPA cyberattack.* Available at: https://futurescot.com/human-error-caused-by-phishing-email-likely-source-of-sepa-cyberattack/ (Accessed: 6 March 2025).

Jampen, D., Gür, G., Sutter, T. and Tellenbach, B. (2020) 'Don't click: towards an effective anti-phishing training. A comparative literature review', *Human-centric Computing*

and Information Sciences, 10 Available at: https://doi.org/10.1186/s13673-020-00237-7.

Jari, M. (2022) 'A Comprehensive Survey of Phishing Attacks and Defences: Human Factors, Training and the Role of Emotions', *International Journal of Network Security & Its Applications,* 14(5) Available at: https://doi.org/10.5121/ijnsa.2022.14502.

NCSC (2025) *How to spot a scam email, text, message, or call.* Available at: https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams (Accessed: 2 March 20255).

NCSC (2024) *Phishing attacks: defending your organisation.* Available at: https://www.ncsc.gov.uk/guidance/phishing (Accessed: 2 March 2025).

Proofpoint (2024) *2024 State of the Phish: Risky actions, real-world threats and user resilience in an age of human-centric cybersecurity.* Available at: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf (Accessed: 2 March 2025).

Renaud, K., Musarurwa, A. and Zimmermann, V. (2021) 'Contemplating Blame in Cyber Security', *International Conference on Cyber Warfare and Security*. February, 2021. Reading: Academic Conferences International Limited, pp. 309.

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M. and Coventry, L. (2022) 'Phishing simulation exercise in a large hospital: A case study', *DIGITAL HEALTH,* 8, pp. 1–13 Available at: https://doi.org/10.1177/20552076221081716.

Schiller, K., Adamsky, F., Eichenmüller, C., Reimert, M. and Benenson, Z. (2024) 'Employees' Attitudes towards Phishing Simulations: "It's like when a child reaches onto the hot hob"'. *ACM SIGSAC Conference on Computer and Communications Security*, Salt Lake City, UT, USA. New York, NY, USA: Association for Computing Machinery, pp. 4167.

Schneier, B. (2000) *Secrets and lies: digital security in a networked world*. Indianapolis, Indiana: Wiley Publishing.

Segal, E. (2022) '25% Of Workers Lost Their Jobs In The Past 12 Months After Making Cybersecurity Mistakes: Report', *Forbes,* 29 March. Available at: https://www.forbes.com/sites/edwardsegal/2022/03/29/25-of-workers-lost-their-jobs-in-the-past-12-months-after-making-cybersecurity-mistakes-report/ (Accessed: 2 March 2025).

Stalans, L.J., Chan-Tin, E., Moran, M., Hart, A. and Pardonek, J. (2024) 'Being phished and reporting phishing emails: emotional and knowledge antecedents and training gaps', *Journal of Crime and Justice,* , pp. 1–19 Available at: https://doi.org/10.1080/0735648x.2024.2415321.

Tschakert, K.F. and Ngamsuriyaroj, S. (2019) 'Effectiveness of and user preferences for security awareness training methodologies', *Heliyon,* 5(6) Available at: https://doi.org/10.1016/j.heliyon.2019.e02010.

Whitman, M. and Mattord, H. (2019) *Management of information security*. 6th edn. Boston, Massachusetts: Cengage.

Zhang, Z., He, W., Li, W. and Abdous, M. (2021) 'Cybersecurity awareness training programs: a cost–benefit analysis framework', *Industrial Management & Data Systems,* 121(3), pp. 613–636 Available at: https://doi.org/10.1108/imds-08-2020-0462.

GANTT CHART

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors
0		**MSc Project**	**15 wks**	**Mon 19/05/25**	**Sun 31/08/25**	
1		**Literature Review**	**10 wks**	**Mon 19/05/25**	**Sun 27/07/25**	
2		Questionnaire content research	2 wks	Mon 19/05/25	Sun 01/06/25	
3		Project wide research	8 wks	Mon 02/06/25	Sun 27/07/25	
4		**Project Implementation**	**9 wks**	**Mon 26/05/25**	**Sun 27/07/25**	
5		Questionnaire development	2 wks	Mon 26/05/25	Sun 08/06/25	
6		Questionnaire distribution	4 wks	Mon 09/06/25	Sun 06/07/25	5
7		Questionnaire results analysis	1 wk	Mon 07/07/25	Sun 13/07/25	6
8		Methodology development	1 wk	Mon 14/07/25	Sun 20/07/25	7
9		Virtual environment setup	1 wk	Mon 09/06/25	Sun 15/06/25	
10		PhishSim platform development	3 wks	Mon 16/06/25	Sun 06/07/25	9
11		Methodology testing	1 wk	Mon 21/07/25	Sun 27/07/25	8
12		**Write dissertation**	**9 wks**	**Mon 30/06/25**	**Sun 31/08/25**	
13		Introduction	1 wk	Mon 30/06/25	Sun 06/07/25	
14		Literature Review	2 wks	Mon 07/07/25	Sun 20/07/25	13
15		Methodology	3 wks	Mon 21/07/25	Sun 10/08/25	14
16		Results and Discussion	1 wk	Mon 11/08/25	Sun 17/08/25	15
17		Conclusions and Future Work	1 wk	Mon 18/08/25	Sun 24/08/25	16
18		Abstract	1 wk	Mon 25/08/25	Sun 31/08/25	17
19		Referencing	1 wk	Mon 25/08/25	Sun 31/08/25	17
20		Formatting	1 wk	Mon 25/08/25	Sun 31/08/25	17
21		Feedback implementation	1 wk	Mon 25/08/25	Sun 31/08/25	17
22		Proofing	1 wk	Mon 25/08/25	Sun 31/08/25	17