

A Study of whether phishing simulations are effective in educating users identify malicious emails, or do they create a negative impact within the workplace?

Sarah Rule 1810755 | B.Sc (Hons) Computing (Computer Networks and Cybersecurity)

1810755@student.uwtsd.ac.uk

Introduction

Digital Technology is becoming a profound part of everyday life for every individual and organisation. Healthcare Data has significant value and is a potential target for hackers. Phishing is a method of potentially gaining valuable information such as usernames, passwords, and medical data for malicious reasons. Phishing refers to this general approach, in which large amounts of untargeted communications are sent to a wide range of recipients in the hope that the minority will become victims. [1]

The project researches the level of cyber awareness within Digital Health and Care Wales (DHCW) and identify whether there is a requirement for further education in helping to mitigate the possibility of a data breach using phishing simulations as the method.

Testing

A technical solution called ProofPoint was used to gather the data for the evaluation into the level of cyber awareness. The testing consisted of :

- ♦ 3 phishing simulations (Using 2 different templates)
- ♦ Immediate feedback (In the form of a poster)
- ♦ User feedback Q & A session

Analysis

Analysis of the data following the three simulations suggests that DHCW would benefit from further education to improve their knowledge when it comes to identifying malicious emails.

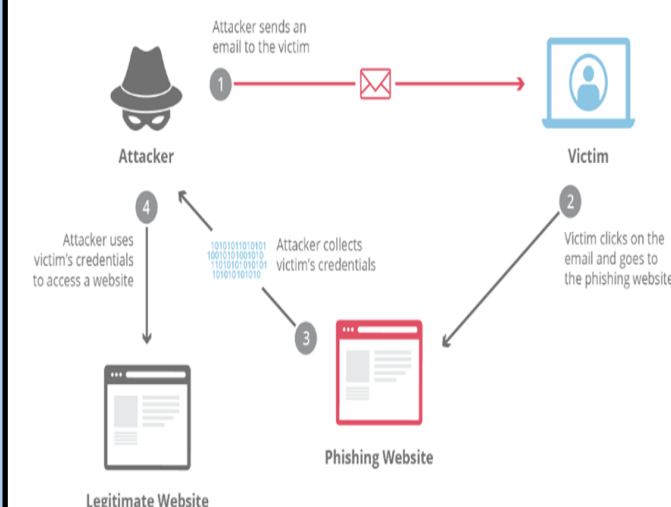
Whilst the data is beneficial to gauge an understanding of the current level of awareness, it is not 100% accurate due to a number of reasons, including:

- ♦ Not all email templates are the same level of difficulty
- ♦ It is unknown whether users who deleted the email knew it was malicious, or they were simply not interested in the content
- ♦ It is unknown how many users were not in work at the time of the simulations

Aim

The main aim of the project is to:

- ♦ Evaluate and Analyse the level of Cyber Security awareness in DHCW
- ♦ Produce and Implement a training plan to improve the overall cyber awareness.



Objectives

The Project objectives are to:

- ♦ Research and analyse current journals and articles and provide critical literature review.
- ♦ Determine a suitable methodology for the project.
- ♦ Conduct a meeting with the Head of Cyber Security to capture the requirements for the applications and determine acceptable expectations.
- ♦ Conduct primary research into the current applications capabilities and identify what the new application needs to include.
- ♦ Evaluate the application by running a series of Campaigns on DHCW users.
- ♦ Evaluate and investigate the impact of the application from a user's point of view.
- ♦ Conduct the project under project management best practice and complete a reflective writing on the project completion.

Conclusion

A full analysis of the data following the three simulations suggests that DHCW would benefit from further education to improve their knowledge when it comes to identifying malicious emails.

User feedback suggested that not all users were happy with the use of phishing simulations to evaluate the awareness, indicating that the use of phishing simulations within the workplace causes a negative effect amongst staff,

"I don't really care to be honest, I don't feel I have the time to check each and every email that comes through, especially when it relating to things I do daily, like use Teams. There are measures in place to sort the problem if it affects me and my laptop so I'm not worried."

(Male, Project Management, NHS)

References

- [1] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: Threats, mitigation and approaches," *BMJ Heal. Care Informatics*, vol. 26, no. 1, Sep. 2019, doi: 10.1136/BMJHCI-2019-100031.
- [2] "What is a phishing attack? | Cloudflare." <https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/> (accessed Jun. 24, 2022).

