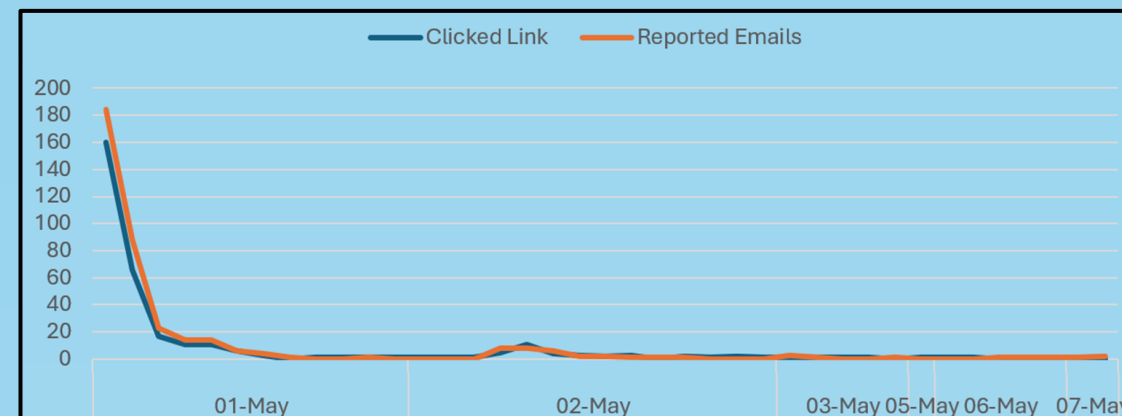


Enhancing Cyber Resilience: Evaluating the Impact of Phishing Simulation Campaigns within Velindre University NHS Trust

Introduction

Over the last few years since Covid-19 phishing attacks have evolved exponentially in complexity, and in amount sent [1], necessitating cybersecurity measures within the VUNHST. Through the creation of phishing campaigns and training material the project will compare campaigns and surveys to gauge if staff have developed skills and knowledge on how to identify and report suspicious emails.

Timeline



Results

Timeline

The timeline shows the duration of the phishing campaigns, an interesting unforeseen result from this was that after day two of the campaign there was almost no interaction from staff. This is due to many variables such as staff receiving a lot of emails and missing this, absence from work, and clinical staff don't use emails as much as admin so may have missed it.

Comparison

These charts show an increase of **22.19%** increase in participation and almost **8%** increase in staff reports between the first and second campaign. Which provides clear evidence that the aim of the project had been achieved. The compromised results were better than predicted, an article that was discussed within the literature review [2], wrote how most organisations result in **20-30%** staff falling for a phishing link.

Aims and Objectives

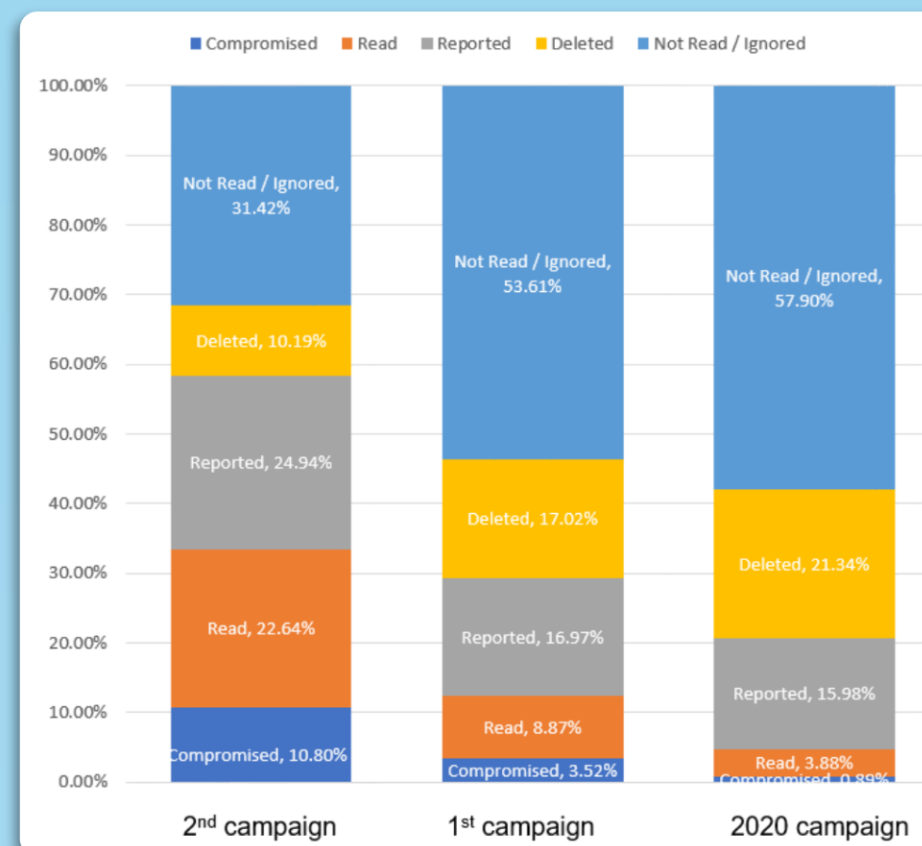
Aim

To enhance cybersecurity awareness and resilience within Velindre Cancer Centre by designing, implementing, and assessing controlled phishing campaigns, and subsequently developing and delivering targeted training materials.

Objectives:

1. Establish Baseline Understanding of Staff Awareness
2. Design and Execution of Phishing Simulation
3. Development and Delivery of Educational Content
4. Evaluation and Reporting

Comparison



Conclusion and future development

Overall, the aims and objectives of the project have been achieved and VUNHST has been extremely satisfied with the results and intend to continue to develop the training material and campaigns while also implementing them into other branches of the Health Board such as Welsh Blood Service and Velindre Head Quarters.

One of the key aspects of the project's success was the variety of training material, creating documents, presentations and PDFs played a fundamental part in staffs accessibility to gaining knowledge. This idea was spawned from information gained within the literature review [3].

References

- [1] AJ Thompson, "NHS Healthcare workers faced a barrage of Phishing attacks during the pandemic", northdoor, 13th August 2020, Available: <https://www.northdoor.co.uk/insight/news/nhs-phishing-attacks/>
- [2] Article, "How to Build a Successful Phishing Simulation Campaign", Terranova Security, 24th February 2022, Available: <https://www.terranovasecurity.com/blog/successful-phishing-simulation-campaign>
- [3] Sunil Chaudhary, Vasileios Gkioulos, Sokratis Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program", Journal of Cybersecurity, 23rd May 2022, Available: <https://academic.oup.com/cybersecurity/article/8/1/tyac006/6590603>