Part 3: Human-Centred Security

Phishing Campaign

Marc Geggan

CMP417: Engineering Resilient Systems

2022/23

Word count: 2,164

**Note that Information contained in this document is for educational purposes.*

Contents

1 INTRODUCTION

Phishing attacks continue to pose a significant threat to organisations worldwide, with threat actors constantly developing new tactics and campaigns to exploit human-centred vulnerabilities. According to the National Cyber Security Centre (2023), as of April 2023, a staggering 20 million phishing scams have been reported, demonstrating the scale of the issue.

These statistics highlight the need for organisations to strengthen their human-centred security and implement appropriate mitigation measures to increase their resilience against phishing attacks. The consequences of falling victim to a phishing campaign can impact organisations in a range of negative ways such as damage to their reputation, disruptive impacts on business operations, and the potential for heavy regulatory fines (CybSafe, 2019).

This report will tackle the real-world challenges that ScottishGlen is facing in terms of human-centred security considering phishing attacks against the organisation. Extensive research and a review of literature on phishing attacks will be carried out to understand the risks posed by uninformed employees. Additionally, research will be carried out on authentication design, exploring different schemes, and carefully evaluating their suitability for safeguarding services within the organisation. The aim of this paper is to present a comprehensive set of measures that mitigate risks and recommend an authentication mechanism that satisfies both security and user-friendliness requirements, taking into account financial constraints of the organisation.

2 HUMAN-CENTRED RISKS

Phishing attacks have been defined by Yeoh et al., (2021) as the process of attempting to obtain personal or compromising information from targets such as account details, financial data, or other details that can be used to gain access to a target network by exploiting human security weaknesses. Organisation employees are usually the main targets of these attacks, which are typically caried out through deceptive communication methods, such as email campaigns or fraudulent websites, aiming to trick individuals into revealing sensitive information or performing actions that compromise the security of the organisation.

The security of an organisations network relies on humans following correct policies and procedures; therefore, we must understand how human factors create security concerns within networks. A research paper published by Goel, Williams and Dincelli., (2021) explain that threat actors take advantage of employee's habits, motives, and cognitive biases to manipulate them into revealing confidential information. According to the research carried out, employees process information on emails or messages quickly, relying on mental models or heuristics that causes them to miss common indicators of a phishing message. This automatic response, coupled with a lack of awareness among employees, often leads to successful targeted phishing attacks. It was also discovered that threat actors exploit human emotions such as fear and greed, and often target specific groups through contextualised spear phishing for more effective results.

The idea of threat actors exploiting human emotions, such as fear and greed, is supported by a paper published by Kim and Kim., (2013). In their study, they explore tactics employed in a typical banking phishing message, which manipulates fear by convincing a user that their account will be blocked unless they select a link and change their credentials. The fear of losing access to something crucial often leads the target to unknowingly handing over their credentials. This type of human exploit is not limited to online banking and can also be applied to organisational settings where threat actors create specially crafted messages to leverage employee's emotions such as fear, greed, trust, or curiosity to extract compromising information from them.

Further human-centred risks were discussed in a paper published by Desolda et al., (2022). The paper revealed that human vulnerabilities exploited in phishing attacks extend further than emotions. It highlighted four other human factors that were exploited by threat actors. Lack of knowledge, awareness, and resources were identified as significant factors, emphasising the need for employee education and guidelines to improve their resilience to attacks. This can be further backed by research conducted by Georgiadou et al., (2021) that revealed 53% of the surveyed employees within the study did not have adequate information or guidelines from their employer regarding cybersecurity. Complacency was also discussed in the paper by Desolda et al., where employee's assumption of being insignificant targets to a threat actor led to negligence of cybersecurity practices and observation. These findings highlight the importance of addressing human factors and implementing mitigations to enhance the organisational resilience to phishing attacks.

3 HUMAN-CENTRED RECOMMENDATIONS

In Dhilon's., (2018) book titled "Information Security, Text & Cases", it is discussed how managing information system security relies on the maintaining of three systems: Formal, technical, and informal. It is highlighted by the author that any misalignment among these three systems can create security problems and expand the human attack surface. Formal controls are a set of policies, procedures, or guidelines created by the organisation that allocate responsibility to employee's and implement rule-based structures for securing access to confidential information. Informal controls focus on increasing awareness and developing a security-conscious environment within the organisation through targeted and tailored education, training, and knowledge sharing with all groups of employees. Technical controls will be discussed further in Chapter 4 – Authentication mechanisms.

In the afore mentioned book it was emphasised that managing information system security requires maintaining formal, technical, and informal systems. One of the crucial components if the formal controls is **anti-phishing training**. By providing employees with tailored training programs, including the use of gamification, organisations can enhance employee awareness and reduce the risk of phishing attacks impacting the organisation. The effectiveness of anti-phishing training can be understood in the study conducted by Mayhorn and Nyeste., (2012). Participants of the study completed questionnaires, cognitive tests, and engaged in role-playing tasks involving email stimuli. The participants were then split into groups and given different levels of training. The results showed that the game training and embedded training groups were less susceptible to phishing emails the second time round, compared to the control group. There was no significant difference between the game training and embedded training groups. However, phishing susceptibility was found to be higher in the second week compared to the first week for all groups, demonstrating the importance of anti-phishing training for increasing the resilience of a company's employees to phishing attacks.

The second proposed layer of mitigation to enhance employee awareness and reduce risk of phishing attacks is the implementation of **software** that is designed to detect and identify malicious emails and warn employees of a possible attack, allowing them to report the email and delete it without interacting with its contents beforehand. There are several software tools and services available to detect and prevent phishing attacks, however this paper will discuss the implementation of Microsoft Office 365 Defender. This software is a cloud-based subscription service that provides protection against various cyber attacks, including phishing campaigns. This software utilises Exchange Online Protection (EOP) to effectively identify and block email-based threats by utilising advanced techniques such as machine learning (Chamberlain, 2019). Defender also contains additional and more advanced anti-phishing features such as impersonation and spoofing detection for specific message senders and domains (Chrisda, 2023). Out of the box, Defender isn't aware of the domains, users, or threats that are sensitive to specific organisations and therefore policies must be created by the organisations IT department. However, the software does allow the company to perform internal phishing campaigns, reducing costs of resilience testing from external companies.

The final proposed layer of mitigation to enhance employee awareness of phishing attacks is introducing **guidance and policies** on top of the staff training. Creating an organisation wide anti-phishing policy will aid in overall cybersecurity posture by outlining how an organisation and its employees can defend themselves from targeted cyber-attacks, including how to identify and report suspicious messages

(eccouncil, 2021). Tools such as GCA's Cybersecurity Toolkit can be utilised to create such policies, offering a structured approach to include a list of rules, guidance, and information. It is crucial that all staff members read, understand, and sign the policy, promoting the importance and awareness of phishing dangers whilst also providing staff with best practices on how to deal with it.

4 AUTHENTICATION MECHANISMS

Securing organisations from cyber attacks is a constant challenge of striking the right balance between security and usability, especially when it comes to authentication mechanisms. According to Nosseir, Connor and Dunlop., (2005), one commonly adopted classification divides authentication into three categories: Something you know, something you have, and something you are. In the first category, **something you know**, users rely on knowledge-based information such as passwords, pins, or memorable phrases. Although these may be easy to remember and widely recognised by users, they are prone to many weaknesses. Firstly, common users of authentication mechanisms do not consider the complexity of their passwords. If an organisations authentication mechanisms lack in password complexity policies, many users select easily guessable and convenient passwords. The handling of passwords is also a security concern, as users often write them down, and can be easily stolen, leading to unauthorised access of systems. Developers tasked with developing code that handles passwords must do so in a secure manner however, history has shown that this task often fails leading to exposed passwords. Finally, authentication methods that use passwords are often susceptible to brute-forcing and password spraying attacks, emphasising the need for further mechanisms such as multi-factor authentication to implement further security checkpoints (Adams et al., 2010).

The second classification of authentication mechanisms is **something you have**. This consists of physical devices or tokens that the user possesses. Examples of this may include smart cards and RFID technologies, USB devices, or digital certificates. Although this method may be considered more secure than standard passwords or pins, they do come with their own vulnerabilities as discussed by Pilson and McElroy., (2015). Within this paper the authors argue that physical mechanisms have certain issues that must be addressed such as the cost incurred by the organisation for purchasing the physical devices. It was also argued that these methods are somewhat inconvenient to users as they must carry and use physical devices which may become disruptive. The risk of loss was also considered, emphasising that loss or stolen devices would give an attacker access to systems. Finally, the issue of scalability was discussed. It was discovered in the study that scaling the use of physical authentication devices across the organisation would pose logistical challenges and greatly increase the overhead of the team implementing them. Given the negatives of physical authentication methods, an alternative approach to authentication taking into consideration useability and effectiveness, is the implementation of authenticator mobile applications as this uses devices that are already carried by employees.

The final classification of **something you are** utilises biometric authentication methods that rely on physical characteristics of the employee such as fingerprints, facial recognition, or voice patterns. This classification is useful for eliminating the need for users to remember passwords or carry physical devices around for authentication, as they themselves are the 'password' however this has major drawbacks and limitations for the organisation. As discussed by Yu et al., (2014) there are privacy concerns as it involves the collection and storing of sensitive biometric information, which has a potential risk of being accessed by threat actors. Additionally, the implementation of biometric devices may incur large costs to the organisation. Changes within the employee's characteristics may also lead to inaccurate results with biometric data. Finally, the complexity of implementing and maintaining these systems and specialised knowledge required creates bigger overhead for management as discussed in the paper.

5 AUTHENTICATION RECOMMENDATION

Considering the previous research of authentication methods around the something you have, know, and are, and the challenges associated with traditional mechanisms such as passwords and physical devices, the implementation of Multi-Factor Authentication (MFA) applications such as Microsoft authenticator is a recommended approach to authentication.

Multi-factor authentication mobile applications offer an additional layer of security and protection for employees within ScottishGlen and combine something they know (randomly generated pin), with something they have (mobile device). The implementation of the Microsoft MFA app brings several positive aspects to the organisation as discussed by Pranata, Nugroho and Yamaki., (2017). The paper considers the application as a low-cost option as the app is free for users with a Microsoft account, making it accessible for low budget organisations. The application was also considered user friendly as it provides an easy-to-use interface, allowing for users to authenticate their identity, coupled with an easy set up process and straight forward configuration, reducing the overhead for the implementing team.

Overall, the adoption of multi-factor authentication mobile applications such as Microsoft Authenticator provides a cost-effective, user-friendly, and secure solution that aligns with ScottishGlens objectives and considers the tradeoff between security and useability as it develops another layer of security for employees whilst utilising a user-friendly interface without introducing additional hardware devices that would need to be carried around by employees. For reference, a wireframe design resembling Microsoft Authenticator app was developed to demonstrate the simplicity and user-friendly interface of a multi-factor authentication app such as Microsoft authenticator providing a user with a generated code, and an app to authenticate the code and user.

REFERENCES

1. National Cyber Security Centre (2023). Phishing: Spot and report scam emails, texts, websites and calls. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/phishing-scams.
2. CybSafe (2019). How can phishing affect a business? [online] CybSafe. Available at: https://www.cybsafe.com/blog/how-can-phishing-affect-a-business/
3. Yeoh, W., Huang, H., Lee, W.-S., Al Jafari, F. and Mansson, R. (2021). Simulated Phishing Attack and Embedded Training Campaign. Journal of Computer Information Systems, pp.1–20. doi:https://doi.org/10.1080/08874417.2021.1919941
4. Kim, D., & Kim, J. H. (2013). Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. Online Information Review, 37(6), 835-850. Available at: https://www.emerald.com/insight/content/doi/10.1108/OIR-03-2012-0037/full/pdf?title=understanding-persuasive-elements-in-phishing-e-mails-a-categorical-content-and-semantic-network-analysis
5. Desolda, G., Ferro, L.S., Marrella, A., Catarci, T. and Costabile, M.F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys, 54(8), pp.1–35. doi:https://doi.org/10.1145/3469886.
6. Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, [online] 35. doi:https://doi.org/10.1057/s41284-021-00286-2.
7. Dhilon, G.S. (2018). Information security : text & cases. Burlington, Vt.: Prospect Press.
8. Mayhorn, C.B. and Nyeste, P.G. (2012). Training users to counteract phishing. Work, 41, pp.3549–3552. doi:https://doi.org/10.3233/wor-2012-1054-3549
9. Chamberlain, N. (2019). Microsoft 365 Mobility and Security - Exam Guide MS-101. [online] Semantic Scholar. Available at: https://www.semanticscholar.org/paper/Microsoft-365-Mobility-and-Security-Exam-Guide-Chamberlain/e95356376d85e88f83f6c3481e23c0e7eb0c9574 [Accessed 22 May 2023].
10. chrisda (2023). Anti-phishing protection - Office 365. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-about?view=o365-worldwide.
11. eccouncil (2021). Security Awareness Training: 7 Steps to Designing an Anti-Phishing Policy for Organizations | Aware | EC-Council. [online] aware.eccouncil.org. Available at: https://aware.eccouncil.org/7-steps-to-designing-an-anti-phishing-policy-for-organizations.html.
12. Nosseir, A., Connor, R. and Dunlop, M. (2005). Internet authentication based on personal history -a feasibility test. [online] ACM Press. Available at: https://strathprints.strath.ac.uk/2754/1/strathprints002754.pdf
13. Adams, C., Jourdan, G., Levac, J. and Prevost, F. (2010). Lightweight protection against brute force login attacks on Web applications. [online] IEEE Computer Society, pp.181–188. doi:https://doi.org/10.1109/PST.2010.5593241.
14. Pilson, C.S. and McElroy, J.C. (2015). A Typology of Authentication Systems. doi:https://doi.org/10.48550/arxiv.1509.00961.

15. Yu, J., Wang, G., Mu, Y. and Gao, W. (2014). An Efficient Generic Framework for Three-Factor Authentication With Provably Secure Instantiation. IEEE Transactions on Information Forensics and Security, 9(12), pp.2302–2313. doi:https://doi.org/10.1109/tifs.2014.2362979.
16. Pranata, S., Nugroho, H. and Yamaki, H. (2017). Analisis dan implementasi protokol otentikasi FIDO U2F. Jurnal ULTIMA Computing, 9, pp.30–35. doi:https://doi.org/10.31937/sk.v9i1.571.