Abertay University®

CMP417 – Engineering Resilient Systems

BSc (Hons)Ethical Hacking 23/24

Human Centred Security

Paul Michael Oates

2001642

02/05/2024

Table of Contents

Table of Figures

1. Introduction

Scottish Glen, a small company in the energy sector has recently received a series of threats after a hacktivist group took exception to comments made by their CEO, employees have reported to the IT team that they have received suspicious emails which they believe to be phishing attacks. The IT team are concerned that it is only a matter of time before someone clicks a link or attachment and exposes the company network.

To mitigate this threat a review of current literature will be undertaken to gain an understanding of phishing attacks and provide recommendations which identify both strengths and weaknesses. To address the concern that some of the company's internal web applications currently don't require employees to authenticate, human centred authentication methods will be designed and discussed. This will develop a defence in depth strategy which prevents lateral movement through Scottish Glens' internal applications making the company more resilient.

2. Human Risks & Recommendations

2.1. Human-centred risks:

2.1.1. Overview

A phishing attack is when an attacker sends a fraudulent email or text message which aims to incite the user to click a malicious link which will download malware such as ransomware or manipulate users to disclose sensitive information (NCSC , 2018). Emails are one of the most popular methods of communication with over 3.9 billion people having email accounts. Collectively, 290 billion emails are sent per day (The Radicati Group., 2023). Due to this, phishing emails prove a popular exploitation method for attackers to gain access to systems, deploy ransomware or other malicious attacks. This was also highlighted by research that was carried out by the Internet Crime Complaint Centre of the FBI (Lozan Mohammed Abdulrahman, 2023).

2.1.2. Propagation

Mohamed Alsharnouby (2015) discovered within "Why phishing still works: User strategies for combating phishing attacks" that only 53% of the users correctly identify phishing attacks even when they were alerted to their presence. Figure 2-1 identifies how phishing attacks can propagate across a network.

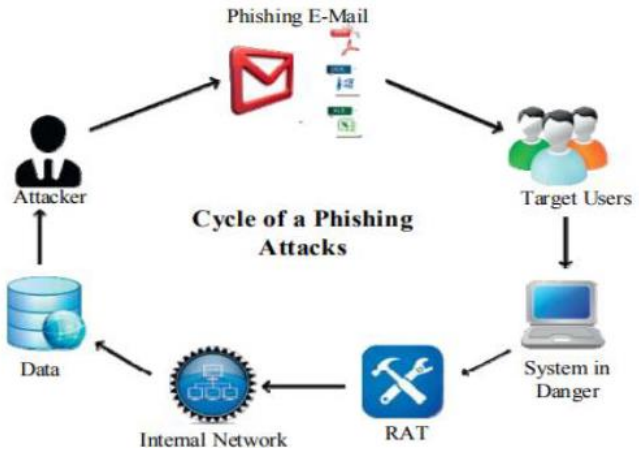

Figure 2-1 Phishing Lifecycle (Mohamed Alsharnouby, 2015)

This details that phishing emails are a prolific and consistent threat even to businesses not under a targeted attack. Regarding Scottish Glen their concerns around hacktivists potentially sending targeted phishing emails is a valid concern.

2.1.3. Psychology

Hoffman & Klein (1992) identify three key differences in the way in which experts and non experts approach events. These are typicality, fine distinctions and past experiences. Within human-centered security experts are able to identify phishing emails quickly and more accurately than non experts. Wash (2020) examined 21 IT experts and their ability to detect phishing emails. The paper highlights that expert users look for inconsistencies, typicality violations, and frame violations. One respondents reasoning is shown below after receiving a email to a birthday party:

"He thought it was unusual that he got an email about it rather than hearing about it in person (a typicality violation). He got an "event not found" error (a frame violation). He noticed the URL didn't go where he expected it to (an inconsistency)." (Wash, 2020)

As seen within the quote, experts identify issues that do not fit the narrative, ultimately making them suspicious. This can be seen in Figure 2-2 which identifies the cues noticed by participants before shifting to be suspicious:

Cue	# Participants
Action Link	8
Typo	3
Suggested by another person	3
Recipients in from line	2
Unusual subject line	2
Attachment	1
URL	1
Unusual information requested	1
Never became suspicious	2

Figure 2-2 The last cue noticed by participants before shifting to be suspicious (Wash, 2020)

These are all risks to Scottish Glen employees as their employees could be unskilled in identifying what a typical phishing attack looks like, unable to spot distinctions within the email, and lack the experience in dealing with phishing attacks.

2.1.4. Demographics

Another risk to Scottish Glen is employee demographics as discussed within, "Experimental Investigation of Demographic Factors Related to Phishing Susceptibility" (Wanru Li, 2020). This report discusses demographics such as age and gender and whether certain groups are more likely to fall for a phishing attack than others. Figure 2-3 identifies the success rate of a phishing link within given demographics:

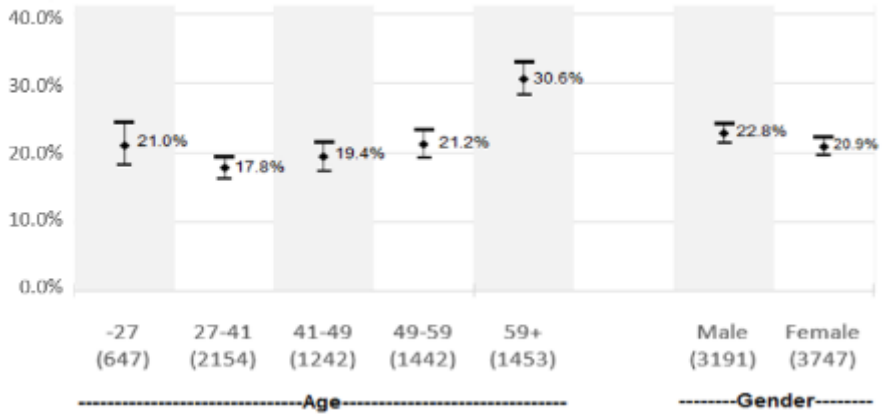

Figure 2-3 click rate by demographic (Wanru Li, 2020)

The findings within this paper identify that the 59+ age group were the most susceptible to phishing emails, however interestingly individuals in the younger age group (27 and under) were more susceptible than those between the ages 27 – 41. The paper also states that the most effective indicator of susceptibility to phishing attacks is those who have been previously phished. (Wanru Li, 2020)

2.1.5. Workload

Another risk that must be addressed is mental health factors such as stress caused by high workload "So Many Phish, So Little Time: Exploring Email Task Factors and Phishing Susceptibility" (Dawn M. Sarno, 2022).

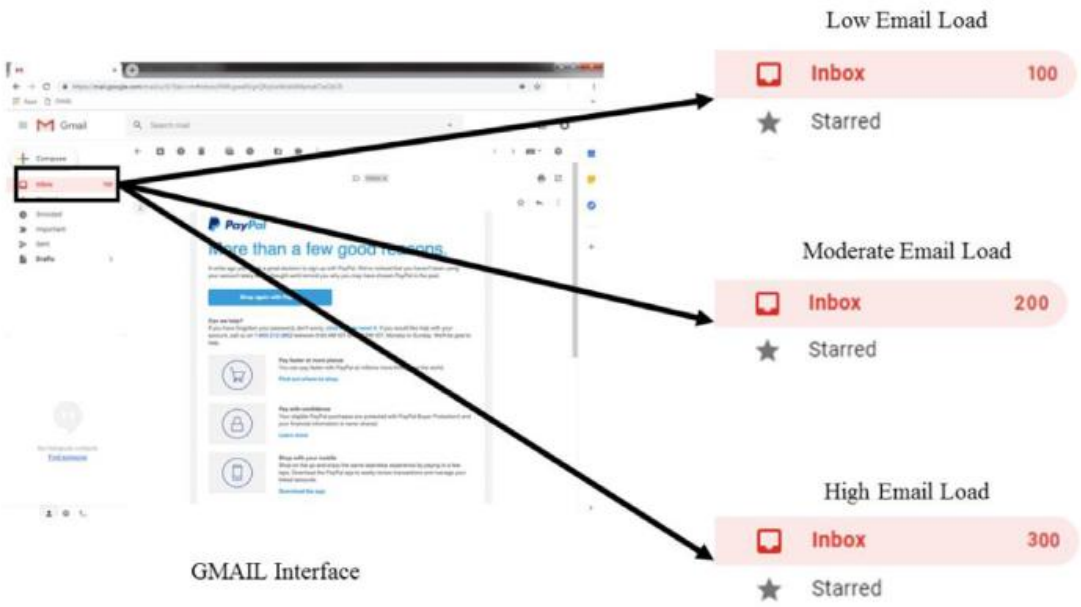

Figure 2-4 Email load (Dawn M. Sarno, 2022)

This paper discusses the accuracy of detecting phishing emails within a simulated workload. Sarno (2022) discovered participants with a high workload did poorly when it came to detecting phishing emails.

2.2. Human-Centred Recommendations:

To reduce the risk of phishing attacks against Scottish Glen, a human centred approach must be adopted. This approach would ensure employees are confident to report security incidents, ask for advice, and be able to mitigate against these kinds of attacks. Through regular testing and training employees would be kept up to date of risks. This will be in addition to any technical approach.

2.2.1. Training

Regular cybersecurity training including phishing training should occur. By covering topics such as attack pattern, techniques used, example phishing messages, attacker intent, and how to report attacks, employees will understand the threats that are out there and how to appropriately report them. However factors such as program quality, apathy, and culture can all affect how successful phishing training can be. (Crowdstrike, 2023)

As discussed within, "Experimental Investigation of Demographic Factors Related to Phishing Susceptibility" (Wanru Li, 2020). Age and falling for previous attacks are good indicators of who are more likely to fall for phishing attacks. This could help employers identify employees who require additional security training. System administrators may also need a further level of security.

2.2.2. Simulated Phishing Attacks

Another method that can be deployed to mitigate phishing attacks is discussed by CrowdStrike (2023), simulated phishing attacks can help novice users to become familiar with these emails by: identify patterns, characteristics and intent (Crowdstrike , 2023). This will likely help novice users develop the same perceptive that experienced IT professionals use as discussed by Wash (2020) and Klien (1992). Figure 2-5 identifies the Microsoft simulated phishing tool:

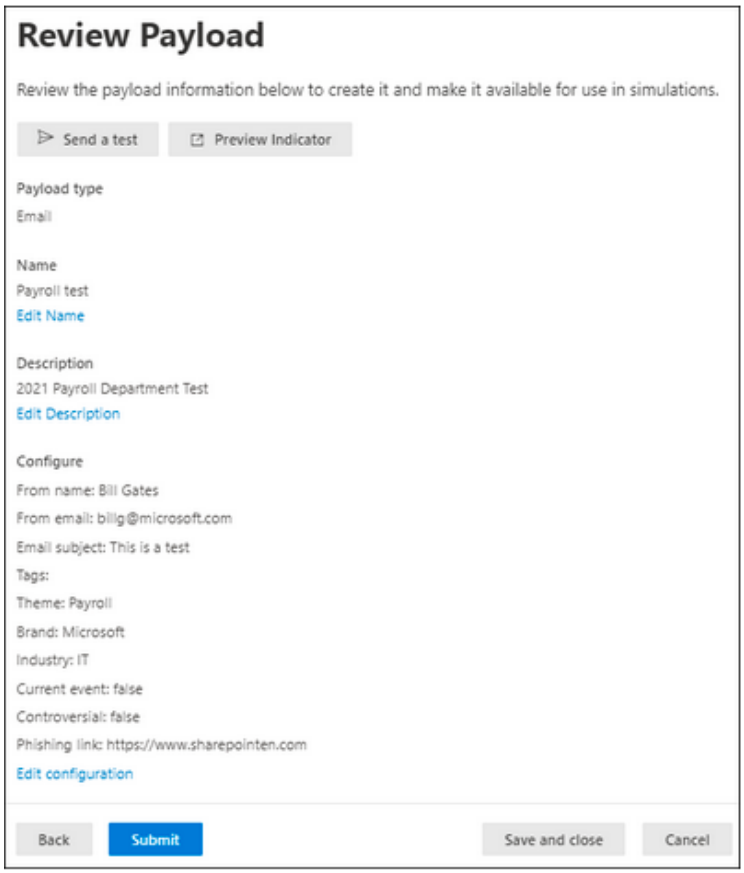

Figure 2-5 Microsoft Simulated Phishing Payload Configurator

However, as discussed by the National Cyber Security Centre (NCSC) phishing simulations can lead to distrust between employees and security teams. Phishing simulations can also create a legal risk as employees failing these can begin to resemble entrapment.

To mitigate this distrust an open and supportive environment where colleagues can ask questions and report with confidence should be developed. This could include information sessions, competitions, and rewards for successful identifications (NCSC , 2018) The NCSC's guidelines as seen in Figure 2-6 show a layered approach to mitigating phishing attacks incorporating human centred and IT solution.

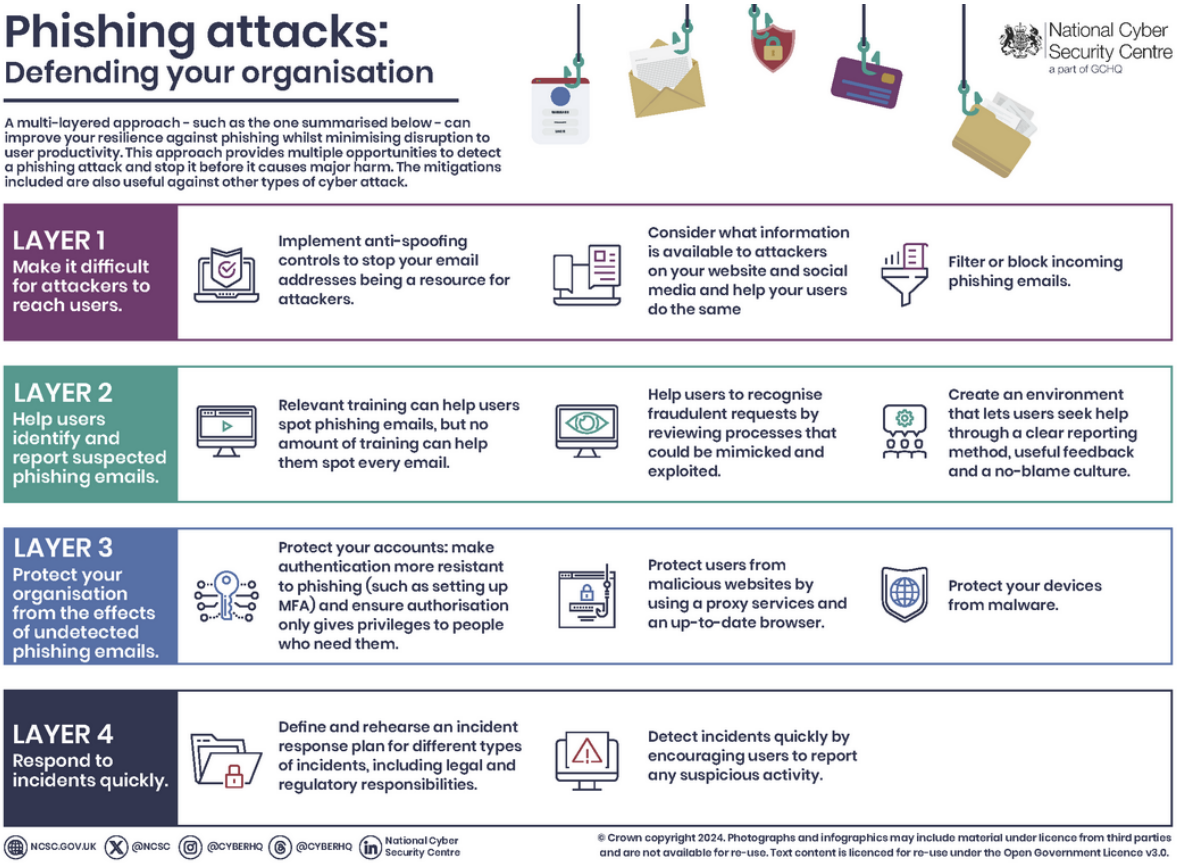

Figure 2-6 NCSC Phishing attacks (NCSC , 2018)

Another solution is to report or ask for advice from IT and cybersecurity professionals who will see phishing emails on a daily basis. As discussed by Wash (2020) when they state that an important population in mitigating phishing attacks are IT experts. One tool that can be deployed by the IT team is the HoxHunt tool, a phishing simulation and reporting system. HoxHunt appears within the browser as a small icon that employees can click if they detect a phishing email. Figure 2-7 identifies the points scoring system:

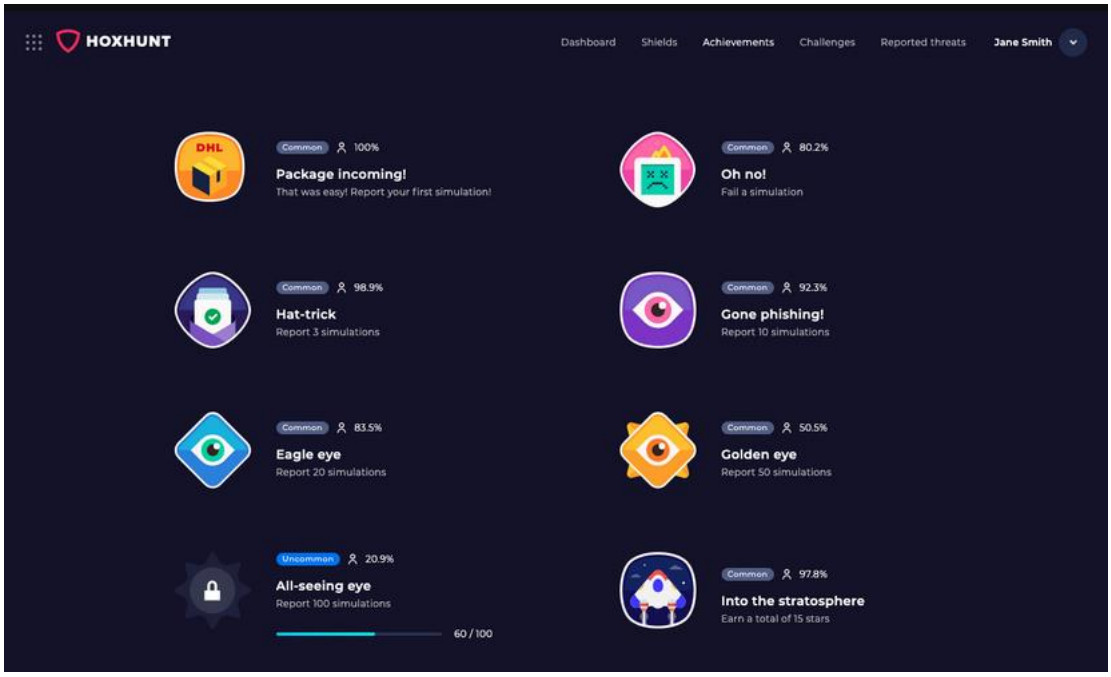

Figure 2-7 HoxHunt (HoxHunt, ND)

HoxHunt sends all employee reported emails to the IT teams for analysis to determine if they are malicious. However IT teams could still become swamped if users are frequently reporting emails.

2.2.3. Conclusion

A robust policy should be developed by Scottish Glen that includes technical and human mitigations including email spam filters, training, multifactor authentication, and an incident response plan. These plans and policies should be kept up to date and reviewed regularly.

3. Authentication Mechanisms & Recommendations

Scottish Glen believe that it is only a matter of time before someone clicks a phishing link, a defence in depth strategy must be deployed to mitigate this, specifically authentication systems should be developed and introduced to the production systems.

3.1. Authentication Mechanisms

“A Usability Study of Five Two-Factor Authentication Methods” discusses two factor or Multi-Factor Authentication (MFA) this requires user’s to present at least two of the following: something they know – a password, something they have – a One Time Passwords (OTP) , or something they are – such as a biometric scan (Ken Reese, 2019) in order to ensure correct identification.

3.1.1. Passwords

As discussed by the NCSC, an average user will have dozens of passwords to remember and users regularly reuse or use insecure passwords, these are easily exploited by attackers. In order to ensure employees use robust passwords businesses can purchase a password management solution. Password managers offer an alternative, more secure, way of coping

with password overload. By implementing a password manager and strong passwords end users follow good password procedures. (NCSC, 2018)

3.1.2. Smart Card Authentication

"A Review Of Authentication Methods" (Nilesh A. Lal, 2016) discusses the various methods of authentication that can be used to keep systems secure, one such method is smart card authentication, as seen in Figure 3-1.

Figure 3-1 Hardware token (Nilesh A. Lal, 2016)

In recent years, technology has evolved and more secure devices have been created such as YubiKeys, a small USB/NFC authentication device. For YubiKeys to work they must be close to or inserted into the device. This provides a second layer of physical security. YubiKeys are used by major organisations as part of their security strategy such as Google (Ken Reese, 2019).

3.1.3. Authentication Apps

A cheaper alternative to this, is a device like a modern phone which has installed a Microsoft authentication app. This method uses Time-based One-Time Passwords (TOTP) to authenticate the user. This however can cause some issues as employees could have under 30 seconds to authenticate (Ken Reese, 2019).

Agata Kruzikova in "Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction" (Agata Kruzikova, 2024) concluded that security is more important than speed for users as employees feel their accounts are secure.

3.1.4. Biometric Authentication

Biometric authentication (something you are) is highly reliable because physical human characteristics are difficult to forge, near impossible to lose, and there is no need to remember anything (Debnath Bhattacharyya, 2009). However ethical considerations of how to keep this data stored and processed arise. Within applications such as Microsoft's Authenticator, it can be configured to request biometric authentication to gain access to the TOTP through fingerprint scan or facial recognition. This method may be appropriate for Scottish Glen as reputable industry techniques are used to keep the data secure.

3.1.5. Conclusion

Scottish Glen should deploy a Multi-Factor Authentication (MFA) system which requires a password (something you know) through a tool such as a password manager. This combined with a TOTP (something you have), which can only be accessed through a biometric scan, (something you are) should provide sufficient security for the day to day running of systems.

Further authentication methods may be required for a handful of employees with elevated permissions, such as the IT team. For this team having a further layer of security through a device such as YubiKeys would improve Scottish Glens security.

3.2. Authentication Recommendations:

3.2.1. Login Page Design

The Scottish Glen login page should be a simplistic standard design including logo, title, username input box, password input box, sign in, and help button. The help button would change depending on the application that the end user is accessing. Figure 3-2 outlines this design:

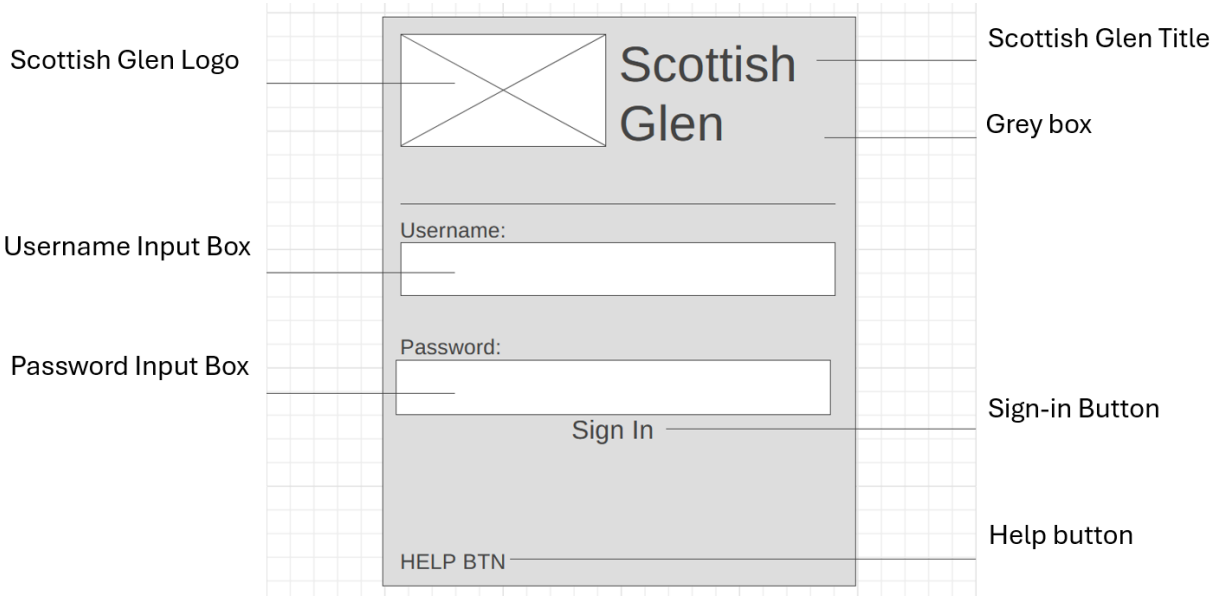

Figure 3-2 Sign in page.

3.2.2. Password Reset Page Design

The password creation and reset system would look like the login system however as the user is changing their password no username would be required. Password rules would be listed here including ensuring passwords are of sufficient length and complexity. An API call to “haveibeenpwned” would be undertaken to ensure the password doesn’t already exist in a password hash table. Figure 3-3 shows the wireframe design of the password reset page.

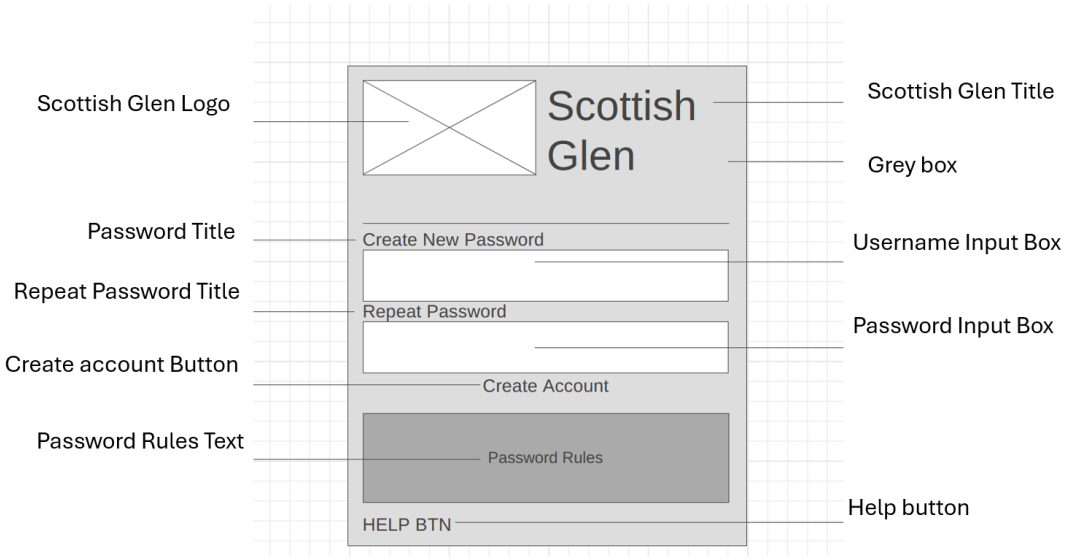

Figure 3-3 Password reset.

3.2.3. *Microsoft Authenticator*

The MFA portion would be covered by Google or Microsoft authenticator as the two are cross-compatible for TOTP codes. As seen in Figure 3-4 the procedure required to login is demonstrated:

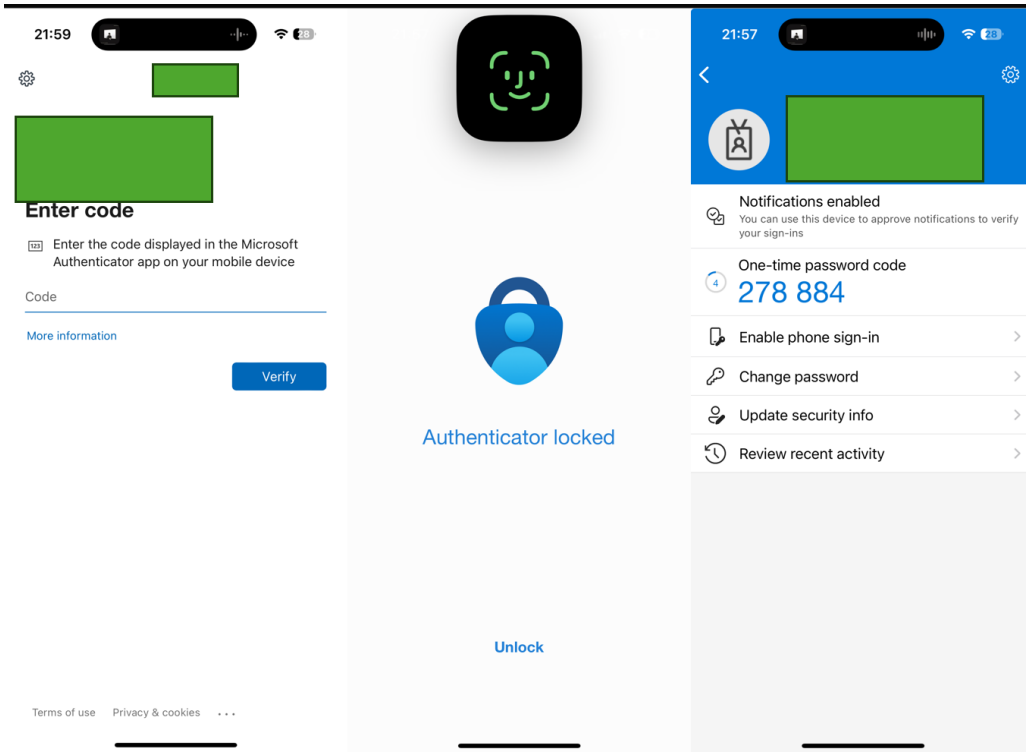

Figure 3-4 MFA login system.

3.2.4. *YubiKeys Page Design*

Figure 3-5 identifies the elevated users prompt. This will be combined with the aforementioned MFA system to provide enhanced authentication to critical systems within Scottish Glen.

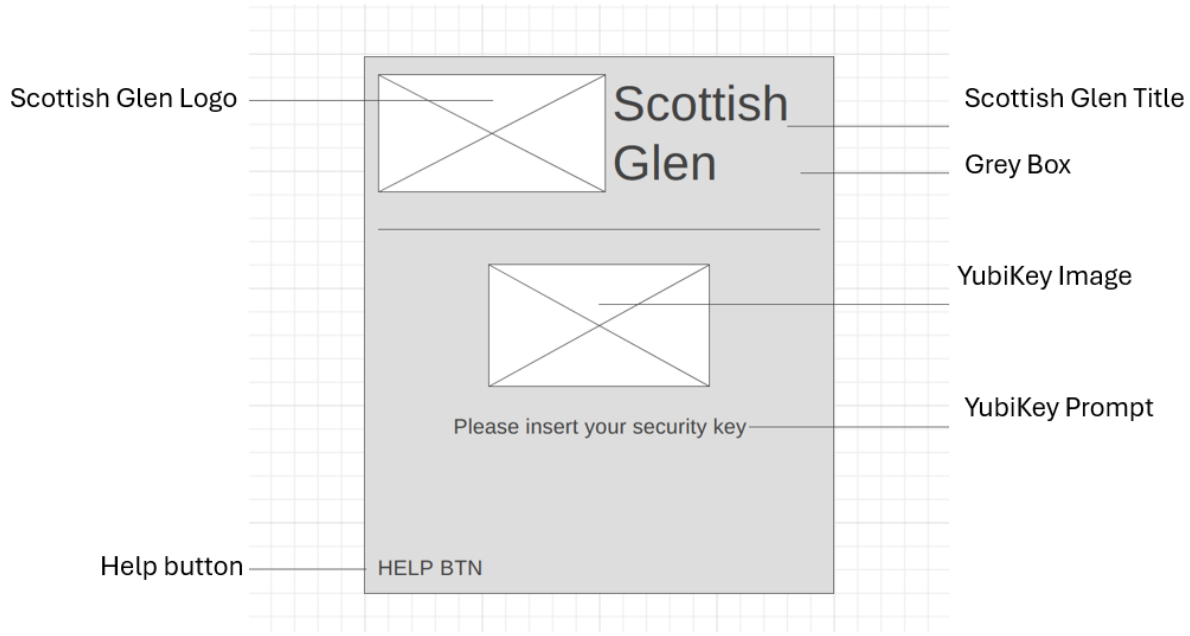

Figure 3-5 YubiKey prompt

By implementing the proposed security changes on Scottish Glens internal facing applications will provide adequate security to prevent lateral movement throughout the businesses infrastructure if a phishing link is clicked.

4. References

Agata Kruzikova, M. M. L. K. L. D. D. S. V. M., 2024. Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction. *Computers & Security,* Volume 138.

Citusdata, ND. *Guide to setting up Yubikey on Google.* [Online]
Available at: https://www.citusdata.com/guides/google_yubikey/
[Accessed 04 05 2024].

Crowdstrike , 2023. *How To Implement Phishing Attack Awareness Training.* [Online]
Available at: https://www.crowdstrike.com/cybersecurity-101/phishing/phishing-attack-awareness-training/
[Accessed 30 04 2024].

Crowdstrike, 2023. *How To Implement Phishing Attack Awareness Training.* [Online]
Available at: https://www.crowdstrike.com/cybersecurity-101/phishing/phishing-attack-awareness-training/
[Accessed 05 05 2024].

Dawn M. Sarno, M. B. N., 2022. So Many Phish, So Little Time: Exploring Email Task Factors and Phishing Susceptibility. *Human Factors,* 64(8), pp. 1269 - 1442.

Debnath Bhattacharyya, R. R. F. A. A. M. C., 2009. Biometric Authentication: A Review. *International Journal of u- and e- Service, Science and Technology,* Volume 2, pp. 13 -28.

Hoffman, R. R. & Klein, G. A., 1992. Seeing the impossible: Perceptual-Cognitive Aspects of Expertise. *Cognitive science foundations of Instruction,* pp. 203 - 226.

HoxHunt, ND. *Collecting Achievements in the Hoxhunt Training*. [Online]
Available at: https://support.hoxhunt.com/hc/en-us/articles/360021398499-Collecting-Achievements-in-the-Hoxhunt-Training
[Accessed 05 05 2024].

Ken Reese, T. S. J. D. J. A. J. C. K. S., 2019. A Usability Study of Five Two-Factor Authentication Methods. *Fifteenth Symposium on Usable Privacy and Security,* pp. 357- 370.

Lozan Mohammed Abdulrahman, S. H. A. Z. N. R. Y. S. J. T. M. G. S. U. H. J., 2023. *Web Phishing Detection Using Web Crawling, Cloud Infrastructure and Deep Learning Framework*. [Online]
Available at: https://jastt.org/index.php/jasttpath/article/view/144/52
[Accessed 2024 04 29].

Mohamed Alsharnouby, F. A. S. C., 2015. Why phishing still works: User strategies for combating phishing attacks,. *International Journal of Human-Computer Studies,,* Volume 82, pp. 69-82.

NCSC , 2018. *Phishing attacks: defending your organisation*. [Online]
Available at: https://www.ncsc.gov.uk/guidance/phishing#section_2
[Accessed 29 04 2024].

NCSC, 2018. *Password administration for system owners*. [Online]
Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
[Accessed 06 05 2024].

Nilesh A. Lal, S. P. M. F., 2016. A Review Of Authentication Methods. *NTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH,* 5(11), pp. 246 - 249.

The Radicati Group., 2023. *Email Statistics Report 2019-2023 Executive Summary*. [Online]
Available at: https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf
[Accessed 29 April 2024].

Wanru Li, J. L. J. P. F. L. G. B. Y. K. B. L., 2020. Experimental Investigation of Demographic Factors Related to Phishing Susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Sciences ,* Volume 53, pp. 2240 - 2249 .

Wash, R., 2020. How Experts Detect Phishing Scam Emails. *Proceedings of the ACM on Human-Computer Interaction,* Volume 4, pp. 1 - 28 .