Part 3. Human-Centred Security

1. Introduction

A number of employees at the energy company, ScottishGlen, have been the recipients of phishing emails, believed to be from the hacktivist group targeting the company. As a result, the IT manager has seen fit to review and recommend mitigation techniques with a focus on the human aspect of the business. Furthermore, A number of the company's web applications also do not employ any degree of authentication, representing a significant security problem. There is limited budget to address this, with a small team of developers being allocated to aid in rectifying the security gap.

To this end, the investigator has been tasked with two primary goals:

- Identify and provide recommendations to improve human-centred security, in order to avoid potential consequences from phishing.
- Identify and provide recommendations to improve authentication security, involving proposing a method that takes into account the situation of the company.

2. Human-centred Risks

The human aspect of cybersecurity is one of the largest potential areas of exploitation when it comes to frequency of attack, with Verizon estimates from the Data Breach Investigations report indicating that 82% of breaches included some form of human element (Verizon, 2022). One of the most prevalent forms of human-centred attack is phishing – phishing is a cyberattack method in which an attacker attempts to trick individuals into revealing personal or sensitive information typically through deceptive emails or websites.

Multiple historical examples of phishing have had significant consequences – these include cyberattacks on the University of California, wherein a phishing email led to a ransomware attack, resulting in the University paying a ransom of 1.14 million dollars (Ogochukwu C & Chinedum E, 2024) or the case of the Austrian aerospace company FACC where an email posing as the CEO successfully tricked an employee into sending 42 million Euros to an attacker's bank account (Ding, et al., 2019).

Understanding what makes individuals vulnerable to phishing is critical in preventing incidents. Many factors can increase the susceptibility of an employee to phishing, with a systematic review of 163 research articles identifying some of the following areas (Althobaiti & Alsufyani, 2024):

- Job responsibility, IE: Somebody being a manager tends to result in more caution and less susceptibility.
- Demographically, younger individuals are generally less likely to fall for phishing than their older counterparts.
- The department of the employee plays a role, wherein employees from social departments are more susceptible than those in technological departments.

Recognising these vulnerability factors, some institutions have taken proactive steps to mitigate risk. In response to their phishing incident, the University of California implemented mandatory annualised cybersecurity training for both staff and students and had monthly phishing simulations that provided immediate feedback. These initiatives led to a 60% reduction in successful phishing attempts over two years, demonstrating the tangible impact of consistent, practical training measures.

While a lack of knowledge and information are often considered to be a reason for the success of phishing attacks, some research disagrees with this and suggests that current phishing training still leaves 23% - almost a quarter – of all individuals susceptible to phishing attacks, with commonly employed methods such as annualised training and immediate feedback being insufficient for sustained protection (Marshall, et al., 2024). This review presents a well-founded critique of many studied phishing training methods, with it finding significant methodological issues with a large amount of research in the field in relation to elements such as:

- Research being conducted over short periods of time
- Experimental conditions being contrived, indicating that while knowledge has been gained, they are not tested under long-term and naturalistic conditions
- Some methods, such as gamification, lacking vigorous evidence that validates their effectiveness

This level of critique highlights the difficulty in selecting effective, evidence based interventions that offer long-term solutions.

3. Human-centred Recommendations

As research indicates, no one method is entirely successful and phishing requires a multi-layered set of mechanisms to effectively mitigate as many risks as possible. This can also be called the “Swiss cheese model.”, meant to imply that an attacker has to go through multiple interventions (represented by a layer) before successfully making it to the other side.

An ideal multi-layered approach that is feasible for ScottishGlen would combine a short period of high-intensity, engaging learning, led either by an instructor or the IT manager, with the opportunity to practice the skills developed. It’s important that this period of learning be engaging and brief such that employees don’t experience information overload (so-called “Cyber fatigue”) (Reeves, et al., 2021) , and the previously mentioned research by Marshall, et al. indicates that intense training programs had a generally higher success rate. This is a human-intensive and perhaps more costly method of phishing training when compared to an example such as e-learning, but the benefits for retention are likely worth it – as one successful session with small refreshers may ultimately end up being more cost-effective than multiple e-learning sessions that are required due to failed retention.

This can be reinforced and supplemented by periodic phishing simulations to maintain long-term cyber awareness and ensure knowledge is retained, especially when research indicates more intense campaigns with a higher volume of simulations generally result in a lower phishing click-through rate (Gordon, et al., 2019). This system could be programmatically implemented, requiring minimal oversight once initially set up. Feedback should be provided immediately after clicking the simulated link, as research indicates this reduces susceptibility to follow-up phishing emails (Bender, et al., 2024). Decisions could also be made based on demographic factors. For example, given that employees in social departments are more susceptible, targeted simulations that mimic realistic scenarios could further personalise and strengthen defences.

This approach addresses several of the methodological concerns raised in recent literature by prioritising realistic conditions, sustained engagement, and feedback rooted in practical action.

4. Authentication Mechanisms

Authentication mechanisms have been identified as a key area for improvement within the company to enhance the security of internal web applications. While username and password entry forms remain one of the most common authentication methods, a growing number of alternative approaches are gaining prominence as organisations seek stronger and more resilient security.

Authentication is often classified into various “factors” – which is where the popular “2 factor” or “multi factor” authentication comes from. These factors are:

- Something you know – Refers to knowledge-based credentials, such as a password or PIN code
- Something you have – Refers to a physical token, commonly a phone or secondary device – and in more secure cases, something like a Yubikey.
- Something you are – Refers to biometric authentication, something intrinsic to personhood, such as facial recognition, voice or fingerprint.

When employing these, three additional elements must also be evaluated – typically identified as usability, deployability,and security – for example, a three-factor authentication system would represent very high security, but has low usability because of the inconvenience it causes the user. A two-factor authentication system will likely be more secure than a single factor, but may be harder to deploy for a small team and may require a secondary application such as an app or the use of another service like Azure or an API – adding potential cost and development time (Bonneau, et al., 2012). An example of this kind of assessment performed against a large number of schemes can be seen below in Figure 1.

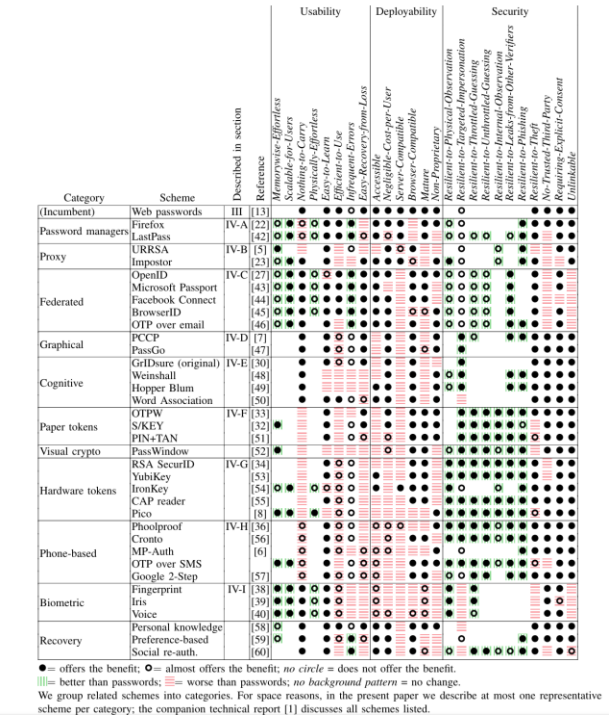

Figure 1 - A comparison of password schemes and their relative usability, deployability and security (Bonneau, et al., 2012)

The balance of these features can be determined based on the contextual elements of what it is being applied to: A bank or healthcare app is likely to employ two-factor authentication as security is worth the potential inconvenience, whereas an online game may only employ knowledge-based

authentication because login is required to be performed frequently (necessitates high usability) with relatively low risk if compromise occurs. Other perhaps overlooked considerations relate to elements such as privacy involving “something you are” with biometric data being highly sensitive.

5. Authentication Recommendations

On account of the fact that ScottishGlen is in the energy sector, even though it is currently a small company – security is of the utmost importance as it represents critical infrastructure and is therefore a potential target for advanced adversaries, beyond the scope of the current hacktivist group. Based on this, it makes logical sense to implement multi-factor authentication – this will undoubtedly increase the cost and required development time but when compared with the cost of a potential breach, it is likely to be a preferable choice. The two factors should likely be a combination of something you know, and something you have – as research indicates that biometrics offer high usability but middling security benefits, with some of the usability elements assessed such as “nothing to carry” being essentially negated by the fact most people carry a phone at all times anyway. Something you are, IE: biometrics also introduces a variety of privacy concerns, which for a business may incur other costs and require additional legislative adherence (GDPR)

The “something you know” factor should be a standard password entry, representing a first line of defence. The insecurity of passwords is a well-known problem, but this can be mitigated by a variety of factors such as mandatory complex passwords in line with updated NIST guidelines (Choong, et al., 2024), adhering to the “should” portions that indicate ideal standards – rather than “shall” – indicating the bare minimum. This includes elements such as a minimum of 15 characters, acceptance of all Unicode characters and no requirement for composition (IE: No requirement for a capital). This can be aided by advocacy for the usage of password managers, as it will result in individuals making their passwords longer due to the lack of remembrance being required. A corresponding email/username should also be required.

The ”something you have” feature should take the form of an authenticator app in combination with a one time password. This app should likely not be proprietary, as a variety of good options already exist and it would reduce deployability significantly, taking time to develop. Authenticator apps are a preferable alternative to other forms of “something you have” as a phone is something most people inherently keep on them, relative to card-based or Yubikey-based authentication (Yubikeys are themselves potentially expensive to provide). Assessment does indicate that SMS based One Time Passwords are overall preferable to app based one time passwords but are undoubtedly less deployable and may be costly. The platform should probably take the form of Google Authenticator, as it is readily accessible and has comprehensive documentation, increasing deployability over other identified options backed by research. This is a reasonably industry-standard implementation of two-factor authentication employed by a variety of businesses, such as banks and universities, indicating it's reliability and acceptance.

A wireframe example for this design can be seen below in Figure 2:

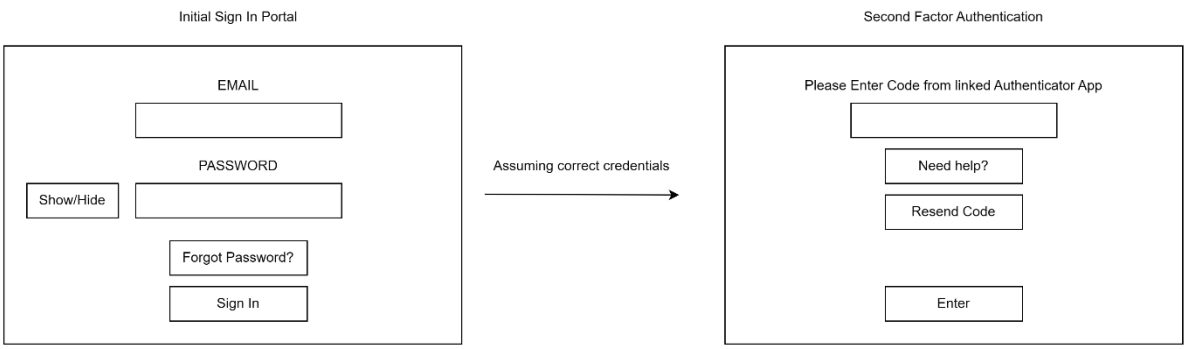

Figure 2 - Example Wireframes Detailing First and Second Factor Authentication

Several design considerations were made:

- The Show/Hide password button is a trade-off between security and usability, as it reduces resilience to observation but significantly reduces the risk of incorrect password entry.
- Remembering the device is not offered at any point, as sign in will persist through the session – which if it is considered to be a working day, should not require multiple sign-ins. This usability reduction is considered to be worth it.
- Self-service password recovery is a potential security risk but it would require breaching of the email of a known user, which is deemed an unlikely scenario. The tradeoff between time saved relative to security risk is considered worth it.
- A “Need help?” link that navigates to a page explaining the setup and usage of the authenticator should be added, increasing usability for users who are not familiar with MFA (Multi Factor Authentication)

The IT Manager recommends subsequent preliminary testing within ScottishGlen, potentially employing the Software Usability Scale (Soegaard, 2024) or other quantitative measure to assess design prior to implementation, with a sample size of at least 5 to ensure the significant majority of usability problems are correctly detected (Virzi, 1992).

References

Althobaiti, K. & Alsufyani, N., 2024. A review of organization-oriented phishing research. *PeerJ Computer Science,* Volume 10.

Bender, S., Horn, S., Loewenstein, G. & Roberts, O., 2024. Phishing feedback: just-in-time intervention improves online security. *Behavioural Public Policy*, 11 September , pp. 1 - 13.

Bonneau, J., Herley, C., Stajano, F. & van Oorschot, P. C., 2012. *The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes.* San Francisco, IEEE.

Choong, Y.-Y.et al., 2024. *Digital Identity Guidelines.* [Online]
Available at: https://doi.org/10.6028/NIST.SP.800-63b-4.2pd
[Accessed 7 May 2025].

Ding, Y., Luktarhan, N., Li, K. & Slamu, W., 2019. A keyword-based combination approach for detecting phishing webpages. *Computers & Security,* Volume 84, pp. 256-275.

Gordon, W. J. et al., 2019. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association,* 26(6), p. Pages 547–552.

Marshall, N., Sturman, D. & Auton, J. C., 2024. Exploring the evidence for email phishing training: A scoping review. *Computers & Security,* Volume 139.

Ogochukwu C, O. & Chinedum E, A., 2024. Awareness of Phishing Attacks in Institutions of Higher Learning: A Review of Types and Technical Approaches. *International Journal of Research and Innovation in Applied Science,* Volume IX, pp. 309-333.

Reeves, A., Delfabbro, P. & Calic, D., 2021. Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open,* Volume 11.

Soegaard, M., 2024. *System Usability Scale for Data-Driven UX.* [Online]
Available at: https://www.interaction-design.org/literature/article/system-usability-scale?srsltid=AfmBOorBeQKWPBkbSUgsK39HHJsCa6aIieP6UYRcN4HhORpAKJ2Dhds0
[Accessed 7 May 2025].

Verizon, 2022. *Data Breach Investigations Report (DBIR).* [Online]
Available at: https://www.verizon.com/business/resources/T920/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
[Accessed 7 May 2025].

Virzi, R. A., 1992. Refining the Test Phase of Usability Evaluation: How Many Subjects Is Enough?. *Human Factors,* 34(4), pp. 457-468.