Abertay University

Human Centred Security Report

Isaac Basque-Rice

BSc. (Hons.) Ethical Hacking
Abertay University
Dundee, United Kingdom
1901124@abertay.ac.uk

23rd May, 2023

Contents

List of Figures

List of Acronyms

2FA Two-Factor Authentication
PIN Personal Identification Number
RFID Radio Frequency Identification
SMS Short Message Service
WFH Working From Home

1 Human-Centred Resilience

Phishing, the "practice of tricking Internet users [...] into revealing personal or confidential information" (Merriam-Webster n.d.) represents the most common cybersecurity threat vector, with 83% of all attempted cyberattacks in the United Kingdom being initiated with this technique (Department for Digital, Culture, Media and Sport 2022). Employees of the organisation ScottishGlen have been receiving suspicious phishing emails from an as-yet unidentified source, suspected to be the hacktivist group previously targeting the organisation. As a result of these two facts, this report has been commissioned to review the situation by researching methods of improving ScottishGlen's security posture from a human-centred approach.

This process involves a review of the extant literature to isolate both the methods by which phishing attacks can compromise security, as well as to what extent uninformed or ignorant employees are a risk to the organisation's security posture. Once this review is concluded, evidence-based recommendations will be laid out to deal with this issue. These recommendations will focus on ScottishGlen's approaches to reducing the risk posed by humans.

1.1 Human Centred Risks

The threat that phishing attacks pose to the security of ScottishGlen cannot be understated. The use of deceptive techniques in order to gain sensitive information, be it from an individual or an organisation, is relatively simple and therefore commonplace, due to the average person's reliance on the internet in the modern era resulting in complacency, according to Muscanell, Guadagno, and Murphy (2014).

In their paper *"Weapons of Influence Misused"*, the authors identify six principles of social influence, which are as follows. Firstly, *Liking*, the idea that likeable people are inherently more trustworthy. Next *Authority*, the idea that authority figures know better. *Scarcity*, the principle that "scarce objects or opportunities are valuable". *Social proof*, the idea that individuals should follow suit if others are doing something. *Reciprocity*, the concept of returning the favour. Finally, *Commitment and Consistency*, the widely-held belief that if an individual holds to their previous pattern of behaviour, they are somehow inherently trustworthy. Muscanell et al. contend that malicious actors, in their terms 'scammers', frequently stick to these principles and are broadly successful when they do so.

A survey conducted by Georgiadou, Mouzakitis, and Askounis (2022) concludes that Working From Home (WFH), a practice made necessary by the COVID-19 pandemic, contributed to a significant increase in attempted

and successful phishing attacks against a more comprehensive array of organisations. Despite this, the "human factor is still not recognised as a core element of the cyber security chain" and, as can be seen in Figure 1, more than half of employees surveyed who were WFH did not receive any security guidance.

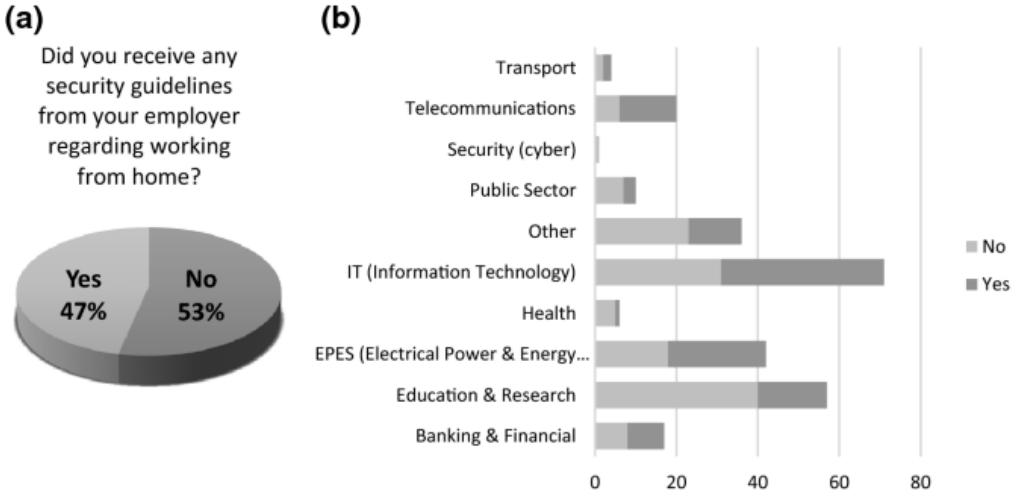


Figure 1: A graph depicting "Security awareness and readiness **a.** overall and **b.** per business domain", adapted from Georgiadou, Mouzakitis, and Askounis 2022.

The key findings by Georgiadou et al. show, amongst other things, the 'violent changes' that businesses have successfully adapted to in terms of other COVID-related disruptions do not necessarily extend into the realm of information security. This highlights the need for organisations, particularly the ones engaging in WFH, to supply their workers with more robust defences and educate them on the risks Phishing attacks may present.

In Sebescen and Vitak's (2017) research article, *"Securing the Human"*, an analysis is performed on a set of employees based on three characteristics (Demographics, Company-Specifics, and Skills-Based), in conjunction with a selection of risk categories, one of which is phishing. The authors observe that those in non-technical positions and younger people with less experience are most prone to phishing attacks. This is congruent with Parker and Flowerday 2020, who found women between 18-25 (young), with lower technical and security knowledge are more susceptible to phishing, and Li et al. 2020, who found that faculty and staff at George Mason University in that same age range were also significantly at-risk, likely due to lack of experience.

1.2 Human Centred Recommendations

In order to mitigate the effects of phishing attacks, it is crucial for a human (or rather employee) centred approach to be taken, in addition to any technical approaches that may already be in place.

As pointed out in the previous section, demographics play a not insignificant part in the likelihood of any individual being phished. As a result, the response must also be catered to different demographics, particularly in terms of both age and technical ability. This is a core finding of literature review *"Don't Click"*, authored by Jampen et al. (2020). The authors advocate for an educational approach, emphasising implementing tools that provide personalised and regular assessment, with a continuous focus on those who fail the phishing tests by clicking faux-malicious links, for example. The improvement this will provide is clear, as repeated exposure to any given thing is a proven method of ensuring readiness for it, and the ability of an employee to spot a malicious link can only improve when this process is undertaken.

This approach, but with additional and particular emphasis on WFH, is in-line with the recommendations of Georgiadou et al. Their recommendations are couched in the more holistic "security culture", which encompasses active participation in simulations, bolstering employee awareness of cybersecurity irrespective of their technical ability, and generally "exploiting each opportunity arisen throughout time and space". Fostering a culture of security within an organisation, e.g., ensuring information security is at the forefront of every employee's mind, reduces the risk of threats across the board (NPSA 2023).

The password management and cybersecurity platform Dashlane (2020) provides information regarding "*How to Run an Effective Phishing Test at Work*" in their blog post of the same name. This post outlines more specifics than the previous articles, providing a four-step approach to planning an effective test. This approach begins with the pre-planning stage, wherein all employees are trained and notified, and the relevant people are engaged. This is followed by a planning stage, where a series of emails or other phishing vectors are developed into a campaign, and no organisation members are excluded. Following the deployment of this campaign is the post-phishing stage, where several metrics, such as clickthrough rates, data leaks, and email reports, are reported on, and employees with less-than-favourable ratings are given additional, personalised training (in line with Jampen et al.'s recommendations) and high performers are rewarded. Then finally, begin planning for the following test.

Finally, a further mitigation mechanism that could be employed is the usage of gamification. As outlined in Wen et al.'s (2019) article,

"What.Hack", the application of game-like concepts into cybersecurity education has demonstrably improved participants' ability to correctly identify attempted phishing attacks (by 36.7% on average, in this case). In the article, the authors outline a specification for a role-playing game wherein the player assumes the role of an employee at an organisation reading through emails and allows the player to allow the email through, mark it as a phishing attempt, or ask an advisor, as seen in Figure 2. The game provides feedback when either a correct or incorrect decision is made in the form of an explanation as to why they were right or wrong. The option (and encouragement) for employees to ask an advisor when they are unsure also aids employees' comfort in asking for help and benefits the organisation's security landscape.

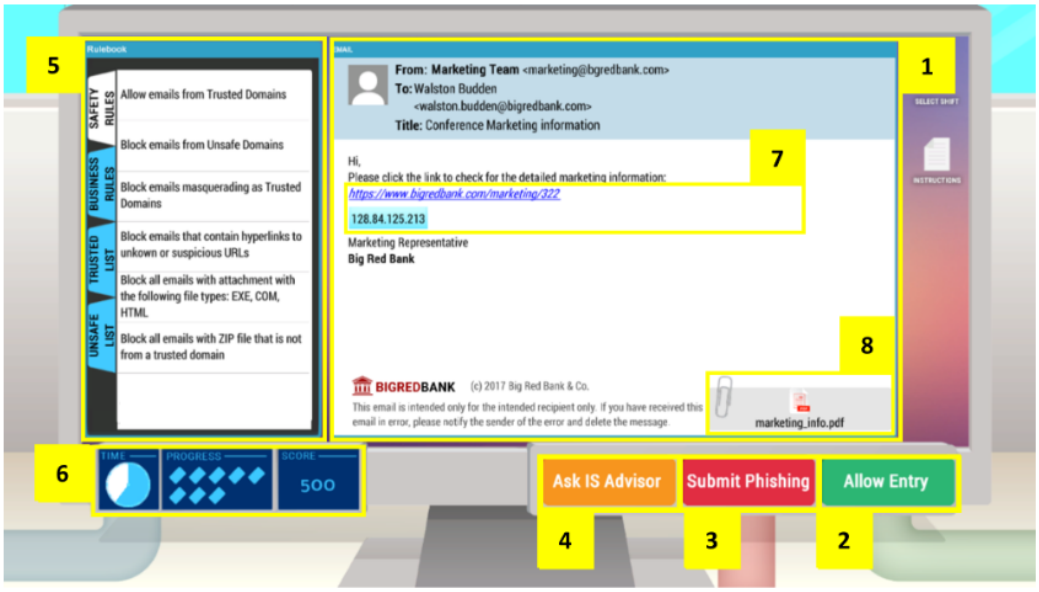


Figure 2: The main screen of *What.Hack*, with different numbered sections highlighted to show the different UI elements. Adapted from Wen et al. 2019.

In ScottishGlen's case specifically, as phishing attempts have already been registered, the mitigations outlined in this section should be implemented as soon as is feasibly possible; however, the fact that all of the (known) attempts so far have been detected as phishing bodes well for the organisation. As ScottishGlen changes its operations over time, be it through changing in size or WFH status, it would be prudent to come back and reevaluate these mitigations. For example, implementing games or professional simulations may be cost-prohibitive and, therefore, may be out of the reach of ScottishGlen, depending on its size and income level.

2 Authentication Design

In addition to the risks posed directly by humans to the organisation, a security concern of a more technical nature has been identified within ScottishGlen. This concern surrounds the reported lack of authentication on some internally-facing web applications. This report recognises the convenience of this approach to the end user and, in devising a solution, will aim to maximise the usability and convenience of the new solution whilst ensuring that ScottishGlen may have confidence in the security of the new solution.

As with the previous section, a literature review will be carried out herein into the different authentication methods, including the design, implementation, and concepts associated with authentication schemas. Following this, a recommendation will be made regarding which authentication schema should be used, taking into account the positives and negatives of this choice and a detailed explanation of the implementation, with a specific focus on security and usability.

2.1 Authentication Mechanisms

Authentication, or "the process of determining whether someone or something is [...] who or what it says it is" (Shacklett 2021), is accomplished via three distinct schemas. These are something an individual **knows**, something they **have**, or something they **are**. Each of these three methods each have different ideal applications and, in turn, different shortcomings that mean they are not to be used in given circumstances.

Lal, Prasad, and Farik's (2016) *"A Review Of Authentication Methods"* suggests that biometrics, the what you **are** schema, is the most secure method of authentication overall. However, it is vulnerable in some instances, and sp the usage of Radio Frequency Identification (RFID) cards (part of the what you **have** schema) in tandem with passwords and Personal Identification Numbers (PINs) (what you **know**) and biometrics will invariably produce the best outcome from a security perspective.

Rui and Yan (2019), in their literature review *"A Survey on Biometric Authentication"*, however, refute this position. They conclude that most existing biometric authentication techniques need help with many issues preventing them from being a truly workable authentication method in their current state. The three areas in which they identify issues are security, privacy, and energy usage.

Regarding the first concern, security, the authors argue that biometrics can often be spoofed easily through pictures of the target's face or copies of their fingerprints. In the second case, they suggest that many of those who

develop biometric systems "did not take potential attacks into account when designing their systems"; thus, if they were to be compromised, people's personal, immutable data would be forever compromised. Finally, and of a more immediate concern, Rui and Yan notes that storage and usage of biometric authentication methods are particularly inefficient and may not be particularly useful in the case of ScottishGlen.

Regarding passwords (and indeed PINs), which are the most well-known member of the something you **know** schema, there are both positives and negatives to this approach. The positives, as pointed out by Pilson (2015) in the article "*Tightly-Held and Ephemeral Psychometrics*", passwords can be easy to remember, flexible, disposable, customisable, and, indeed, are the most common form of authentication today.

The author, however, does recognise the issues with password usage, in particular the tendency for users (especially non-technical ones) to lean towards weaker passwords to reduce the cognitive burden of remembering them, and making simple adjustments when forced to change their password, such as adding a '1' to the end. Additionally, passwords present severe challenges to those with cognitive difficulties, such as dyslexia (Renaud, Johnson, and Ophoff 2021), which results in coping strategies, such as making simple passwords, that are unsound from a security perspective.

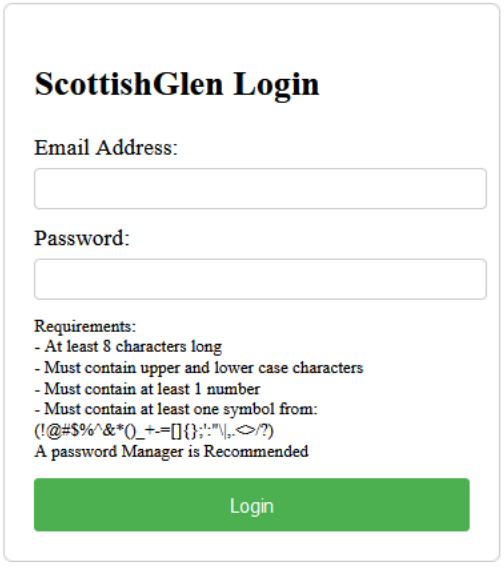
Both papers offer password managers as a partial solution, which is apt, as many concerns about a tendency towards simple passwords and a lack of ability to remember them can be alleviated by the generation and storage of strong passwords that password managers provide. However, these solutions have their drawbacks. Password managers provide a single point of failure, resulting in not only the primary issue that, if a user forgets their password to the password manager, but they are also locked out of everything; many password managers can be cryptographically unsound, resulting in efficient brute-forcing methods to be derived (Ziegler et al. 2014). As such, they would need a secondary form of authentication to ensure a secondary point of failure before hackers could access the accounts.

Finally, the something that a person **has** schema could be implemented in this case. An excellent example of this (to be used with another schema) is the concept of Two-Factor Authentication (2FA), where you have a phone, email address, or hardware token. Many rudimentary forms of 2FA currently send a user attempting to authenticate a short code, typically six digits, to either an email address or specified phone number through the Short Message Service (SMS) protocol. This is a problem because if malicious actors have access to the target email or SMS, they can bypass the 2FA easily (Alharbi and Alghazzawi 2019). Therefore, a superior option is the authenticator app, which uses the user's phone's existing security measures (PIN, biometrics,

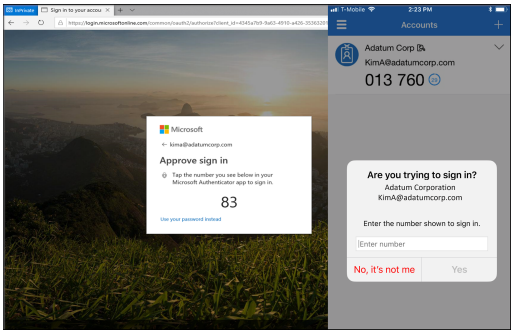
etc.) to authenticate a user account previously associated with that phone on account creation. These apps benefit from being more accessible (Lake 2021).

2.2 Authentication Recommendations

Regarding what authentication methods should be implemented in ScottishGlen's case, a mix of a strong password bolstered by a password manager and 2FA through an authenticator app appears ideal. Figure 3 shows both a mock-up for the login page with the rules and recommendations for the passwords listed underneath (3a), and an example screenshot of what Microsoft's Authenticator looks like when authentication is required, (3b). Note that Figure 3a contains text outlining password rules; this is purely for the benefit of this report and will not be present in the actual login form, as a malicious actor could use it to enumerate passwords.



(a) An Example Login Page for ScottishGlen



(b) An example of a sign-in method in Microsoft Authenticator. Adapted from Hall 2023

Figure 3: Examples of the recommendations for authentication in the case of ScottishGlen, a simple login screen and an Authenticator app.

There will be Microsoft Authenticator, which will be integrated into the (presumably) existing Microsoft suite of services. In this solution, every employee should have access to a phone that meets the security standards of ScottishGlen, either their phone or a company phone. This ensures a layer of

protection for the organisation from malicious intruders attempting to steal credentials and encompasses the something you **have** schema. As well as this, optionally, Authenticator can also cover the something you **are** schema, as it has facilities for confirming a user based on the recognised biometrics within the phone.

The something you **know** schema will be implemented with a standard password login form but with strict regulations on the kind of password that can be created and an overt recommendation that a password manager be used. If uptake herein is too low, options such as an organisation-wide, mandated password manager must be explored.

References

Alharbi, E. and Alghazzawi, D. (June 30, 2019). "Two Factor Authentication Framework Using OTP-SMS Based on Blockchain". In: DOI: 10.14738/tmlai.73.6524.

Dashlane (Mar. 7, 2020). *How to Run an Effective Phishing Test at Work*. Dashlane. URL: https://dashlaneblog.wpengine.com/phishing-test/ (visited on May 22, 2023).

Department for Digital, Culture, Media and Sport (2022). *Cyber Security Breaches Survey 2022*. GOV.UK. URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 (visited on May 20, 2023).

Georgiadou, A., Mouzakitis, S., and Askounis, D. (June 1, 2022). "Working from Home during COVID-19 Crisis: A Cyber Security Culture Assessment Survey". In: *Security Journal* 35.2, pp. 486–505. ISSN: 1743-4645. DOI: 10.1057/s41284-021-00286-2. URL: https://doi.org/10.1057/s41284-021-00286-2 (visited on May 22, 2023).

Hall, J. (Mar. 16, 2023). *Microsoft Authenticator Authentication Method - Microsoft Entra*. URL: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app (visited on May 23, 2023).

Jampen, D. et al. (Aug. 9, 2020). "Don't Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review". In: *Human-centric Computing and Information Sciences* 10.1, p. 33. ISSN: 2192-1962. DOI: 10.1186/s13673-020-00237-7. URL: https://doi.org/10.1186/s13673-020-00237-7 (visited on May 22, 2023).

Lake, K. (July 29, 2021). *MFA Accessibility: Evaluating Different MFA Factors*. JumpCloud. URL: https://jumpcloud.com/blog/evaluating-the-accessibility-of-different-mfa-factors (visited on May 23, 2023).

Lal, N. A., Prasad, S., and Farik, M. (Nov. 25, 2016). "A Review Of Authentication Methods". In: *International Journal of Scientific & Technology Research*. URL: https://www.semanticscholar.org/paper/A-Review-Of-Authentication-Methods-Lal-Prasad/797708bd4f854a125ec20865d4b7be76a1aa4740 (visited on May 23, 2023).

Li, W. et al. (2020). "Experimental Investigation of Demographic Factors Related to Phishing Susceptibility". In: Hawaii International Conference on System Sciences. DOI: 10.24251/HICSS.2020.274. URL: https://hdl.handle.net/10125/64015 (visited on May 22, 2023).

Mentis, H. M., Madjaroff, G., and Massey, A. K. (May 2, 2019). "Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–13. DOI: 10.1145/3290605.3300573. URL: https://dl.acm.org/doi/10.1145/3290605.3300573 (visited on May 23, 2023).

Merriam-Webster (n.d.). *Phishing*. Merriam-Webster Dictionary. URL: https://www.merriam-webster.com/dictionary/phishing (visited on May 18, 2023).

Muscanell, N. L., Guadagno, R. E., and Murphy, S. (2014). "Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams". In: *Social and Personality Psychology Compass* 8.7, pp. 388–396. ISSN: 1751-9004. DOI: 10.1111/spc3.12115. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/spc3.12115 (visited on May 21, 2023).

NPSA (Feb. 27, 2023). *Security Culture — NPSA*. URL: https://www.npsa.gov.uk/security-culture (visited on May 22, 2023).

Parker, H. J. and Flowerday, S. V. (June 15, 2020). "Contributing Factors to Increased Susceptibility to Social Media Phishing Attacks". In: *SA Journal of Information Management* 22.1. ISSN: 1560-683X, 2078-1865. DOI: 10.4102/sajim.v22i1.1176. URL: http://www.sajim.co.za/index.php/SAJIM/article/view/1176 (visited on May 22, 2023).

Pilson, C. S. (Sept. 5, 2015). *Tightly-Held and Ephemeral Psychometrics: Password and Passphrase Authentication Utilizing User-Supplied Constructs of Self*. DOI: 10.48550/arXiv.1509.01662. arXiv: 1509.01662 [cs]. URL: http://arxiv.org/abs/1509.01662 (visited on May 23, 2023). preprint.

Renaud, K., Johnson, G., and Ophoff, J. (Oct. 26, 2021). "Accessible Authentication: Dyslexia and Password Strategies". In: *Information and Computer Security* 29.4, pp. 604–624. ISSN: 2056-4961. DOI: 10.1108/ICS-11-2020-0192. URL: https://www.emerald.com/insight/publication/issn/2056-4961 (visited on May 23, 2023).

Rui, Z. and Yan, Z. (2019). "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification". In: *IEEE Access* 7, pp. 5994–6009. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2889996.

Sebescen, N. and Vitak, J. (2017). "Securing the Human: Employee Security Vulnerability Risk in Organizational Settings". In: *Journal of the Association for Information Science and Technology* 68.9, pp. 2237–2247. ISSN: 2330-1643. DOI: 10.1002/asi.23851. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.23851 (visited on May 22, 2023).

Shacklett, M. E. (2021). *What Is Authentication?* In collab. with L. Rosencrance. Security. URL: https://www.techtarget.com/searchsecurity/definition/authentication (visited on May 23, 2023).

Wen, Z. A. et al. (May 2, 2019). "What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. New York, NY, USA: Association for Computing Machinery, pp. 1–12. ISBN: 978-1-4503-5970-2. DOI: 10.1145/3290605.3300338. URL: https://doi.org/10.1145/3290605.3300338 (visited on May 23, 2023).

Ziegler, D. et al. (2014). "Do You Think Your Passwords Are Secure ? Analyzing the Security of Android Password-Managers". In: URL: https://www.semanticscholar.org/paper/Do-You-Think-Your-Passwords-Are-Secure-Analyzing-of-Ziegler-Rauter/909e89fa9377b30b1b0d324416605bae9fedb932 (visited on May 23, 2023).