|  |
| --- |
| ASP.NET Vulnerability Assessment  Part 3: Human-centred Security  Mikolaj M. Mroz  2003114  BSc (Hons) Ethical Hacking, 2023  CMP417: Engineering Resilient Systems 1 |

|  |
| --- |
| School of Design and Informatics  Abertay University |

Contents

[Context 2](#_Toc135770029)

[Human-Centred Resilience 2](#_Toc135770030)

[Human Centered Risks 2](#_Toc135770031)

[Recommendations 4](#_Toc135770032)

[Pre-interaction Software 4](#_Toc135770033)

[Post-interaction Software 4](#_Toc135770034)

[Bespoke Education and Testing 5](#_Toc135770035)

[Reporting 5](#_Toc135770036)

[Authentication 5](#_Toc135770037)

[Authentication mechanisms 5](#_Toc135770038)

[Authentication Recommendations 8](#_Toc135770039)

[Knowledge 8](#_Toc135770040)

[Ownership 9](#_Toc135770041)

[Biometrics 9](#_Toc135770042)

[Conclusion 9](#_Toc135770043)

[Bibliography 11](#_Toc135770044)

[Appendix 13](#_Toc135770045)

[Appendix 1 – Diagrams 13](#_Toc135770046)

[Appendix 1.1 – Desktop login wireframe 13](#_Toc135770047)

[Appendix 1.2 – Phone login wireframe 14](#_Toc135770048)

# Context

In this final part of the investigation, two literature reviews are conducted into the various mechanisms the client can employ to help mitigate the risks associated phishing attacks and authentication technologies. The aims of this case study are to discuss these mechanisms in the form of a critical evaluation and to design an appropriate means of authentication, particularly regarding usability, user experience, and security based on findings from the literature review. The study then concludes with the design of a user-friendly and secure authentication method.

# Human-Centred Resilience

End users have often been cited as being the weakest link within cybersecurity breach prevention and mitigation (Schneier, 2000). A company which spends its budget entirely appropriately on cybersecurity systems and sets them up precisely as required may still be vulnerable to a slew of different attacks through commonly used attack vectors such as emails, messages, and downloads. Typical security systems are not able to account for these vectors in a fully effective manner, and therefore require human intervention, which can potentially be a great benefit to system security.

## Human Centered Risks

On July 15th 2020, a group of hackers successfully gained access to numerous high-profile accounts on Twitter by posing as members of Twitter’s own IT help-desk employees (Schneier, 2020). By directing an unknowing twitter employee to a phishing site identical to that of the official Twitter VPN login page, they were able to steal administrative credentials, log themselves in, and steal almost $118,000 in Bitcoin (12.86 BTC) from various accounts (New York State Department of Financial Services, 2020). This event highlights the consequences of insufficient in-company protocols on educating employees to identify and prevent phishing attacks, as well as the worrying developments in believable targeted phishing scenarios (spear-phishing).

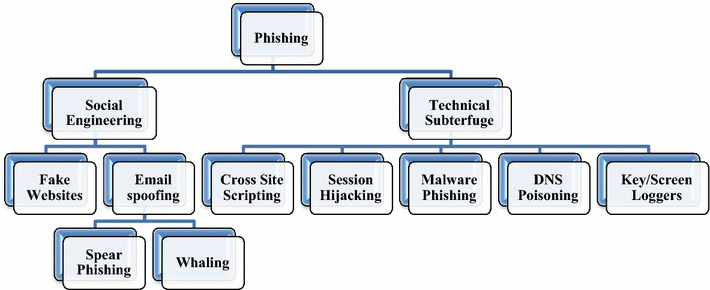


Figure - The various classes of phishing attacks (Gupta, et al., 2018)

Twitter’s hack isn’t the only such event in recent years either, the recent war in Ukraine has prompted hackers to formulate false donation, advance fee fraud, and account validation schemes, targeting internet users around the world on individual and enterprise levels (Shevchenko, et al., 2022). These recent events in particular demonstrate the highly adaptable nature of phishing attacks only adding to the danger they already present in generic spam mail schemes. Shevchenko et. al. discusses human nature as the main reason for these attack’s successes.

An investigation by A. Baillon et. al. (2019) demonstrates the efficiency of various methods in helping people identify and prevent phishing attacks from taking place, with information provision lowering the number of subjects falling for phishing scams by 7% and simulated experience improving this number further to 9%. The study concludes by saying both methods are valid measures to improve employee awareness and knowledge. As a further development, Vayansky & Kumar (2018) suggest a three-pronged approach – detecting the phishing attempt before it reaches a user, detecting it once the link or download has been clicked, and to educate the user, finding that a mix of the three significantly improves phishing awareness and prevention.

These findings are supported by a report by S. McElwee et. al. (2018), which found that repeated exposure to targeted behaviour-based simulations may help in preventing attacks from taking place. This research is particularly important as victims are generally found to be more likely to click on bespoke, targeted messages than generic phishing attempts (Rizzoni, et al., 2022). In this same report, Rizzoni et. al. found that generic phishing emails may often be filtered out by currently available spam detection systems integrated into modern email clients, further demonstrating the importance of custom, targeted simulations.

## Recommendations

The following section assumes that the target group of employees to whom the risks apply have received no security awareness training. This allows for a broader discussion of human-centred recommendations which can be applied where relevant on a by-person basis.

### Pre-interaction Software

The first part of the solution proposed by Vayansky & Kumar uses software to detect phishing attacks before a user even interacts with the communication. This can be implemented in the form of a carefully controlled company-wide email spam filter ideally paired with a machine-learning based filter to dynamically detect anomalies in received network packets, emails, and adverts. Based on the outcome of this check, the software may either detect an anomaly and remove it entirely, clearly flag it as potentially harmful, or, if it is deemed safe, allow it to be interacted with by employees. This greatly reduces the risk of employees clicking on or falling for phishing attacks by removing it outright before an employee has any chance to fall for it.

### Post-interaction Software

Another tool may be implemented into this security system which detects the phishing attempt after an employee has interacted with a harmful link. This adds a second layer of security for the employees and is expected to further reduce the chances of someone navigating a falsified site if a phishing link is clicked. By implementing a defence-in-depth approach, each additional system will theoretically reduce the risk of a cyberattack as the chances of a phishing attempt successfully evading each subsequent defence are greatly reduced.

### Bespoke Education and Testing

Implementing regular mandatory education and testing exercises for employees allows teams to identify weaknesses in company-wide phishing attack detection. Moreover, it allows for employees to be kept up-to-date on the latest cyberattack prevention and mitigation methods. As discovered by S. McElwee et. al. and A. Baillon et. al., these tests must not be generic and should be realistic for maximum effect in the sense that they are relevant to current world events, utilise a believable website design or interface all the while making use of the information presented during the educational phase.

### Reporting

Using this newly gained knowledge, anyone who has discovered a potential phishing attempt must take the time to report it to the appropriate authorities. In the UK, suspicious emails should be forwarded to ‘report@phishing.gov.uk’ and messages to 7726, whereupon a National Cyber Security Centre team will investigate it. This aims at helping identify newly released scams in an ever-evolving field of cyber scams, in turn allowing those at risk to be further educated about what to look out for and for software tools to better identify incoming threats.

# Authentication

As important of a role as employees have in preventing cyberattacks, a significant amount of emphasis remains placed on the authentication systems in place to help further reduce the attack surface.

## Authentication mechanisms

Authentication is the act of proving one’s identity with the aim to prevent unauthorized access into buildings, devices, software, and other restricted locations. Authentication methods can typically be narrowed down to three common factors:

Something you know (Knowledge) – A pattern one can memorise.

Something you have (Ownership) – A physical authentication device.

Something you are (Biometrics) – A unique biological feature.

A person sitting at a desk with a computer

Description automatically generated with low confidence

Figure - A diagram displaying the various forms of authentication within MFA. (Ometov, et al., 2018)

A combination of these three factors is known as Multi-Factor Authentication (MFA) and utilises a defence-in-depth approach to improve security with each added step, reaching a 99% cyberattack prevention rate according to Microsoft’s Director of Identity Security (Weinert, 2019). While MFA can help prevent cyberattacks, this figure is greatly misleading. Typical MFA implementations can be bypassed by attackers through phishing, an attack vector which made up 83% of all business cyber threats in the UK in 2022 according to the UK Department for Digital Culture, Media, & Sport’s Cyber Security Breaches Survey (2022). Thus, extra precautions must be taken on top of MFA to prepare systems against cyberattacks to their fullest extent, and companies should not rely on MFA alone to prevent cyberattacks.

An article by J. Still et. al. (2017) proposes a modern set of guidelines for the creation of a secure authentication mechanism. The report demonstrates the importance of various factors for the design of an authentication process, ensuring all users are as fully protected as possible. In terms of usability, it is recommended that at least 90% of users should be able to complete the authentication process (Schneidermann, 2000), taking into consideration various aspects of accessibility pertaining to cognitive, perceptual, and physical weaknesses. This means that any individual lacking in any of these abilities should not be at a disadvantage. A study from the University of Glasgow (Renaud & Just , 2010) found that asking the user to memorise a picture was a much more effective method compared to the typical textual challenge question, with image-based cues showing a 13% improvement in memorability.

Risk awareness is typically found in individuals who lack the necessary knowledge or motivation to perform the necessary risk analysis of acts such as sharing or reusing passwords. A balance must be found as to not inconvenience the user into using a less secure password but also to prompt the user to generate a password that will take a considerable amount of time for attackers to solve (Abbott, et al., 2018).

Clearness and usability form the last of the guidelines for an appropriate authentication process, citing unclear communication of password requirements. When it comes to usability, the authors of the guidelines suggest that login screens should have support for copying and pasting and password manager support. No academic proof exists to show that including these workflow aids compromise the security of the authentication model in any way. Instead, they aid in employee workflow, particularly in situations where many usernames and passwords must be managed. Bold, clear visuals are also a necessity, aiding those with poor eyesight, smaller screens, and physical disabilities.

## Authentication Recommendations

Based on the literature review into various authentication guidelines, the following recommendations can be made for the development of a secure and inclusive authentication process for each factor of MFA.

See Appendix 1.1 for a desktop authentication wireframe and Appendix 1.2 for a diagram of a mobile phone login wireframe. Note the spacing, sizing, and language used to be as accessible as possible. When developed, the colour contrast must be easily viewed at a distance.

### Knowledge

When asking for the user to generate a password, ensure the following criteria are met:

* The password is over 8 characters in length.
* Remove the upper limit of password length.
* Prevent the use of names or usernames within passwords.
* Make MFA necessary.

Failure to comply with these regulations has the potential to impact the user’s memorisation of their password, prompting them to reuse an old one which greatly undermines authentication security (Abbott, et al., 2018).

If a user forgets their password and a backup system is necessary to make them prove their identity, refrain from using textual memory cues and instead, make use of pictures to improve the user’s memorisation and reduce the risk of this backup information being guessed or found out by attackers.

During account creation and login, remind the user about the dangers of sharing and reusing a password, using language that any reading age can understand. In other words, minimise the use of jargon in this text to make it legible by users of all ages and abilities.

### Ownership

A smartcard + PIN combination is recommended here as it requires the user to have something physical (a smartcard) and know something (a pin). However, asking the user to remember too many things, such as a PIN and a password, may negatively affect their ability to successfully authenticate themselves. To prevent this, a handheld token generator may be used. These are small devices that offer the benefits of a smartcard and PIN combination without requiring the user to remember an additional set of numbers.

An important thing to note is that by removing the PIN from needing to be memorised, all the attacker needs to do to gain access to the system is to hold the token itself. However, a system could be put in place to keep track of the tokens entered, as well as the username. While this does not prevent the attacker from entering, it allows for easier identification of timeframes and suspects within the logs in the event of a breach.

### Biometrics

In terms of pure accuracy, iris scans have been reported to be the best choice (Bhattacharyya, et al., 2009). However, due to their inherently intrusive nature, a fingerprint scanner may be determined to be the better choice, as it does not sacrifice security and shows only a marginal increase in error rates over other options (Clark, 2016). When paired with MFA, it creates a robust and reliable login mechanism for employees.

# Conclusion

In conclusion, several solutions exist to identify dangerous incoming communications, but it is up to the end user to determine the most secure course of action based on their discretion. The incorrect or uninformed choice in this situation has the potential to severely undermine the security of the company, and therefore relevant measures must be taken to train employees appropriately on the situations they may come across and how to respond.

The proposed ways to combat this aim to improve human-centred resilience, combine pre-interaction, post-interaction, and education methods to alleviate the inherent risks of human-centered resilience. To produce an accompanying accessible and secure authentication environment, several factors were considered including usability, risk awareness, memory cues, and workflow. The resulting model combines these factors into an MFA-based system.

# Bibliography

Abbott, J. E., Calarco, D. & Camp, L. J., 2018. *Factors Influencing Password Reuse: A Case Study.* Washington, TPRC46.

Baillon, A. et al., 2019. *Informing, simulating experience, or both: A field experiment on phishing risks,* San Francisco, California: PLOS ONE.

Bhattacharyya, D., Ranjan, R., Alisherov, F. A. & Choi, M., 2009. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology 2.3,* pp. 13-28.

Clark, M., 2016. *Iris Recognition Scanners vs. Fingerprint Scanners: Compare and Contrast.* [Online]   
Available at: https://www.bayometric.com/iris-recognition-scanners-vs-fingerprint-scanners/  
[Accessed 23 May 2023].

Gupta, B. B., Arachchilage, N. A. G. & Psannis , K. E., 2018. Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems,* Volume 67, pp. 247-267.

McElwee, S., Murphy, G. & Shelton, P., 2018. *Influencing Outcomes and Behaviors in Simulated Phishing Exercises.* St. Petersburg, Florida, IEEE, pp. 1-6.

New York State Department of Financial Services, 2020. *Twitter Investigation Report,* Albany, New York: New York State Government.

Ometov, A., Bezzateev, S., Mäkitalo, N. & Andreev, S., 2018. Multi-Factor Authentication: A Survey. *Cryptography 2018*, 5 January.

Renaud, . K. & Just , M., 2010. *Pictures or Questions? Examining User Responses to Association-Based Authentication.* Glasgow, HCI.

Rizzoni, F., Magalini, S. & Coventry, L., 2022. Phishing simulation exercise in a large hospital: A case study. *Digital Health,* Volume 8.

Schneidermann, B., 2000. Universal Usability. *Communications of the ACM,* 43(5), pp. 84-91.

Schneier, B., 2000. *Secrets and Lies: Digital Security in a Networked World.* 15th Anniversary ed. Hoboken, New Jersey: Wiley.

Schneier, B., 2020. *On the Twitter Hack.* [Online]   
Available at: https://www.schneier.com/blog/archives/2020/07/on\_the\_twitter\_.html  
[Accessed 23 May 2023].

Shevchenko, H., Stopochkina, I. & Babenko, I., 2022. Peculiarities of phishing threats and preventive measures in the conditions of war in Ukraine. *Theoretical And Applied Cybersecurity,* 4(1).

Still, J. D., Cain, A. & Schuster, D., 2017. Human-centered authentication guidelines. *Information and Computer Security,* 25(4).

UK Department for Digital Culture, Media, & Sport, 2022. *Cyber Security Breaches Survey 2022,* London: UK GOV.

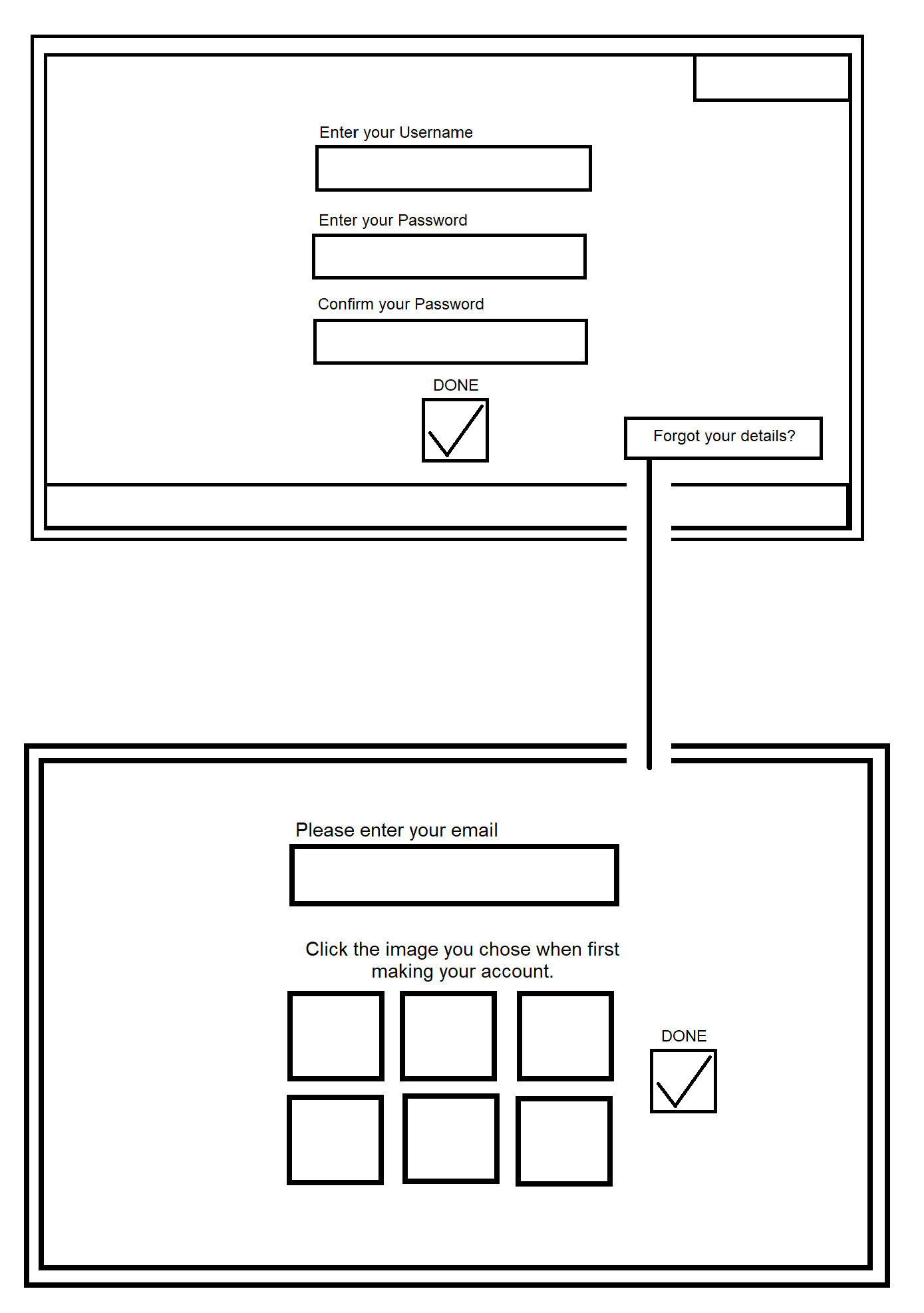
Vasyansky, I. & Kumar, S., 2018. Phishing – challenges and solutions. *Computer Fraud & Security,* 2018(1), pp. 15-20.

Weinert, A., 2019. *Your Pa$$word doesn't matter.* [Online]   
Available at: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984  
[Accessed 23 May 2023].

# Appendix

## Appendix 1 – Diagrams

### Appendix 1.1 – Desktop login wireframe



### Appendix 1.2 – Phone login wireframe

