Human-Centred Security

Adam Board
2005335

1 Introduction

Scottish Glen have requested a review of the current situation with phishing attacks as several employees have received phishing emails that appear to be from a hacktivist group. Scottish Glen have also asked for a recommendation regarding a multi-layered set of mechanisms to mitigate the chance of an employee falling for a phishing attack.

Currently Scottish Glen's internal web application does not need employee authentication to access the contents, which is considered a risk to the organisation. The recommendation for an authentication mechanism must be feasibly produced by in-house developers as there is a limited budget for addressing the lack of authentication.

2 Human-Centred Risks

Phishing is a social engineering technique that aims to influence the target into revealing sensitive information such as usernames, passwords, and financial information. The stolen credentials are used to gain unauthorised access to a user's account for malicious purposes (Alabdan, 2020). Typically, the phishing websites or emails aim to mislead users into believing they are a legitimate organisation by illegally utilizing a public or trustworthy organization's images and resources in an automated pattern, which aids in making the user fall victim to the request coming from the phishing website or email (Banu & Banu, 2013).

There are various types of phishing attacks, with most common type of phishing attack being Deceptive Phishing. Deceptive phishing is when an attacker impersonates a legitimate organisation to steal personal information for blackmailing the user into doing malicious activities. (Bhavsar, et al., 2018). Link manipulation is a type of phishing technique where the attacker sends a link that directs a user to a spoofed website. The spoofed website typically impersonates a legitimate website to get unaware users to input their personal credentials into the spoofed website (Bhavsar, et al., 2018).

Research into phishing attacks and the financial damage caused by phishing attacks indicates that humans are the weakest link in securing a system. In 2020, reports shown that over $1.8 billion in losses came from only business email compromise attacks, which far exceeds the amount of financial loss accrued from any other type of cybercrime that year (Jayatilaka, et al., 2021). Attackers utilise phishing to prey on human vulnerabilities, such as invoking emotion and forcing the user into a time-sensitive situation. Attackers focus on invoking fear and anticipation as the key emotions to push them to enter their sensitive information (Sharma & Bashir, 2020).

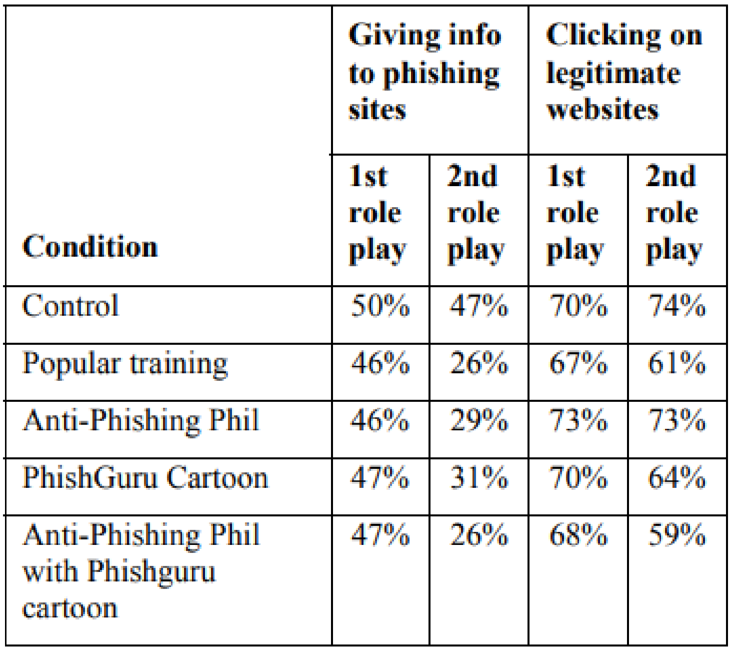
There are a multitude of factors which affect the likelihood of a user falling victim to a phishing attack through email. These factors Include:

- Sender legitimacy.
- Perception about links in emails.
- Need for validation.
- Familiarity of email title and body.
- Professionalism of the email title and body.
- Emotional attachment to email.
- Perceived likelihood of receiving an email.
- Length and granularity of information.
- Previous phishing experiences.
- Sense of security from auxiliary security content.
- Individual habits of a user.

Need for validation was especially important as users would conduct further research on the internet before doing what the emailed requested them to do. However, the attackers creating the email also have access to the same public resources and can create fake but legitimate appearing web applications to give the user a false sense of security and safety (Jayatilaka, et al., 2021).

Phishing attacks are successful because the average user does not know how to identify a phishing attack or understand the severity of the vulnerabilities that can occur from a phishing attack (Sheng, et al., 2010). Research into determining which demographic of users is likely to fall for a phishing attack indicates that users that are less knowledgeable regarding phishing attacks are more susceptible to falling for a phishing attack. users that have knowledge in identifying phishing attacks are much less susceptible to phishing attacks. The results of the research into demographic can be seen in Table 1.

Table 1 Roleplay results by condition for Phishing scenarios (Sheng, et al., 2010)



	Giving info to phishing sites		**Clicking on legitimate websites**	
Condition	**1st role play**	**2nd role play**	**1st role play**	**2nd role play**
Control	50%	47%	70%	74%
Popular training	46%	26%	67%	61%
Anti-Phishing Phil	46%	29%	73%	73%
PhishGuru Cartoon	47%	31%	70%	64%
Anti-Phishing Phil with Phishguru cartoon	47%	26%	68%	59%

3 Human-centred Recommendations

Studies on educating and training staff on how to spot potential phishing attacks have shown that users are less likely to fall for phishing attacks after being trained to spot them. However, providing the staff with short term retention strategies for spotting phishing attacks such as doing a questionnaire or watching a video appears to not be effective in mitigating phishing attacks (Sumner & Yuan, 2019). An organization was audited after their social engineering prevention education to analyse how effective the training was at stopping staff for falling for social engineering attacks. The auditor asked questions such as "What is your username?" and "What is your password?" to 33 different employees, to which 32 employees answered at least one, if not all the questions asked by the auditor. This shows that the training they had received was not effective in the slightest and a different training method should be completed multiple times a year to ensure the staff are vigilant against phishing attacks (Sumner & Yuan, 2019).

Users can be trained through fake phishing emails sent by the organization or a third-party using PhishGuru or similar applications to determine which employees need to go through phishing training. This has shown improved results in spotting phishing attacks because the staff are provided immediate feedback if they have clicked on the mock phishing attack (Kumaraguru, 2009).

A more effective method is through gamification of phishing education. A web-based game named "Anti-Phishing Phil" teaches users about phishing attacks and has shown that users who played the game were able to identify phishing websites immediately after playing the game and also one week later (Alsharnouby, et al., 2015). A mobile version of the game was developed to improve accessibility and compatibility with devices.

While education for phishing attacks is vital, there are other methods of reducing the chances of users falling for a phishing attack. One method includes implementing a cyber-security minded corporate culture to ensure all staff are doing their part to keep an organisation secure. A set of questionnaire results published by a study shows that over 50% of staff did not know how to protect their organisation from cyber-crime, and a further 55% believed they didn't have the necessary technical ability to aid in keeping the organisation secure from cyber-crime (Hadlington, 2018). While creating a cyber-security minded corporate culture is important, there is no set method for doing this, as each organisation is vastly different in ways such as organisation size and age demographic (Hadlington, 2018).

A second method would be to introduce software to detect potential phishing emails and websites before the employee can click on the link. By examining the contents and features of a website or email, software such as "SpoofGuard" can identify if it is a phishing attack. A brief warning is shown to the user to not click on the suspicious email or website with reasons on why it may be a phishing attack (Sumner & Yuan, 2019). However, should a user rely on this type of software, they may fall victim to a phishing attack that is built to bypass these systems.

Since Scottish Glen aims to reduce their human attack surface due to the increase in phishing emails, they should implement a few of the methods mentioned as soon as they can. Not all methods work for every employee so Scottish Glen should select the methods they think would be optimal for their employees.

4 Authentication Mechanisms

Authentication is the process of validating a user's identity before allowing access to a system or network. Typically, to authenticate a user there are three regularly used variables – something you know, something you have, or something you are (Nilesh A. Lal, 2016). An example of something **you know** is usually a password or username; An example of something **you have** is a smart card to authenticate with a physical form of identification; Finally, an example of something **you are** is biometrics such as fingerprint or facial recognition.

Passwords are commonly used as the sole authentication mechanism for accessing resources on a system. However, while passwords are the most popular method of authentication due to ease of use and accessibility, they also have various disadvantages. Some of these disadvantages include users creating weak passwords that can be stolen and reusing those passwords across all their accounts (Renaud, et al., 2014). As mentioned previously, during a study, employees gave their password to an auditor because they were asked for it, which shows the weakness of password security due to the human aspect of password authentication (Sumner & Yuan, 2019). To aid in preventing weak passwords being created, a strict policy can be set in place to force specific requirements such as password length and include special characters.

Smart cards are physical items that are given to employees to allow them to authenticate securely. The smart cards contain a digital certificate embedded within to scan, and is typically paired with a PIN to provide a level of multi-factor authentication. Although, some users will struggle to remember their pin and may write it on the back of the card (Nilesh A. Lal, 2016). This is an issue since the card is a physical object which can be stolen by another individual. If an attacker has the card and the pin is written on it, they would be able to view or edit all resources that the smart card has authentication to access.

Biometric authentication can use various humanistic features about a person such as their voice, fingerprint, facial structure, or retina. Since these characteristics are normally unique to an individual and cannot be easily altered, they are difficult to forge. These systems work by identifying key features from a user's humanistic features and saving these to be compared against for authentication (Dasgupta, et al., 2017). In Figure 1 the seven most common minutiae types used to detect in fingerprint sensors can be seen.

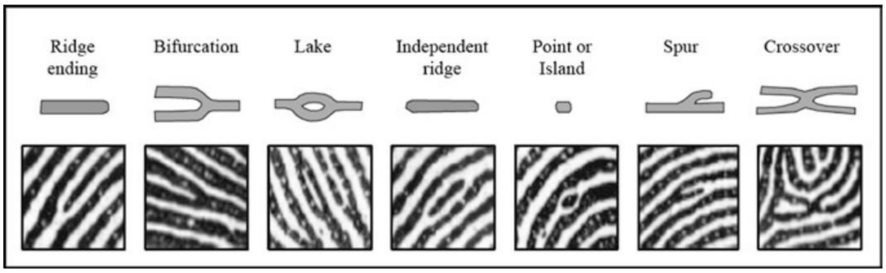


Figure 1 Seven most common minutiae types used to detect in fingerprint sensors (Dasgupta, et al., 2017)

Unfortunately, the technology to implement biometric authentication is expensive and does not factor in accessibility issues which would increase the price of implementation to ensure the authentication method is usable for all employees (Matyáš & Říha, 2002).

Implementing multiple authentication methods will improve the security posture of the organisation at the cost of convenience for employees. If an employee's Single-Factor Authentication (SFA) is compromised without their knowledge, the effects on the organisation can be devastating financially. Multi-Factor Authentication (MFA) solves this problem by providing a layered defence approach to authentication, making it difficult for unauthorised users to gain access to a system even if the first method of authentication has been breached (Dasgupta, et al., 2017). The MFA must be easy to use, reliable and scalable to ensure that it can be pushed to all employees in an organisation (Dasgupta, et al., 2017).

5 Authentication Recommendations

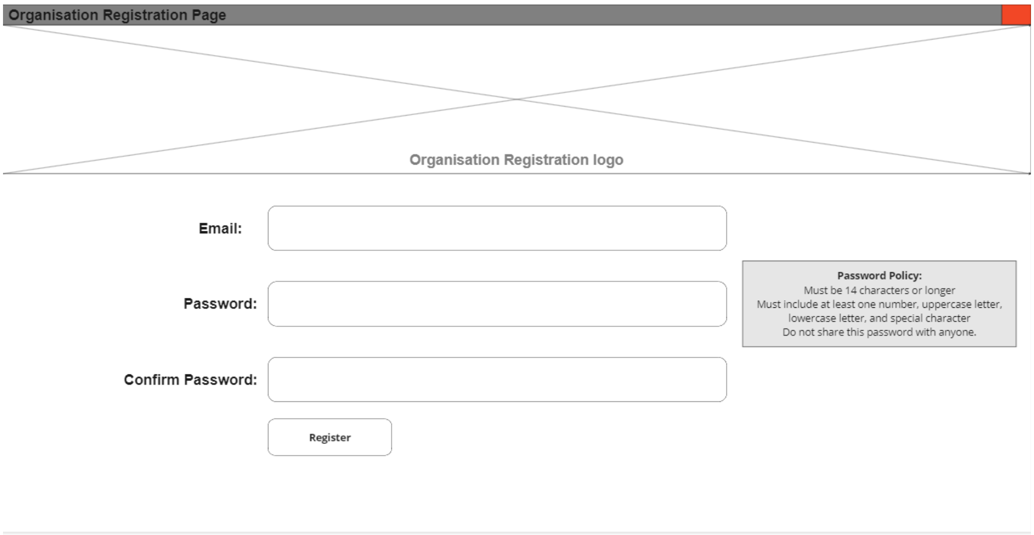
The recommendation that is provided in this report for an authentication mechanism is based on Scottish Glen's needs of usability, security, and feasibility. The proposed method would be to integrate MFA.

To implement MFA, two authentication methods will be integrated together. Passwords will be the first authentication method as the "something you know" variable as mentioned previously. Passwords with strict policies can be tedious for users but provide a simple and cost-effective method of securing an internal web application without a massive overhead. Since passwords are the most popular form of authentication, employees will adjust easily to the new authentication. Since Scottish Glen only want their employees to be able to access the internal resources, the passwords can be linked to their existing organisation accounts.

The secondary authentication method will be based on "something you have". Smartphones are the most cost-effective and accessible solution for secondary authentication. This is because each employee typically has their own smartphone or a work-issued smartphone; Using smartphones reduces the chance of an employee not being able to log-in due to forgetting it when compared to other solutions such as smart cards, as they are a physical item which can be easily forgotten. To ensure that the MFA is easy to use, reliable and scalable, push-based authentication notifications will be used, because it meets all three requirements mentioned (Ken Reese, 2019).

The proposed platform to integrate for MFA would be Duo since it allows 10 free users and only costs $3 extra per month per user above 10 (Cisco, 2023). Once it is integrated, the employees would install the Duo application onto their smartphone and follow the setup process on the application. A major issue would be getting employees to sign-up to the Duo application and activate MFA as users lose a level of convenience if MFA is implemented (Bhanderi, et al., 2023). A solution to this issue would be to make MFA mandatory for logging in to force employees to use MFA even if it is annoying for the employees.

In Figure 2, A registration page has been designed. If pre-existing employee accounts cannot be used to access the internal web application, this registration page would be required to setup new accounts. The page would enforce the NCSC standards for password complexity and length to ensure that the password is following best practices for password security.



Organisation Registration Page

Organisation Registration logo

Email:

Password:

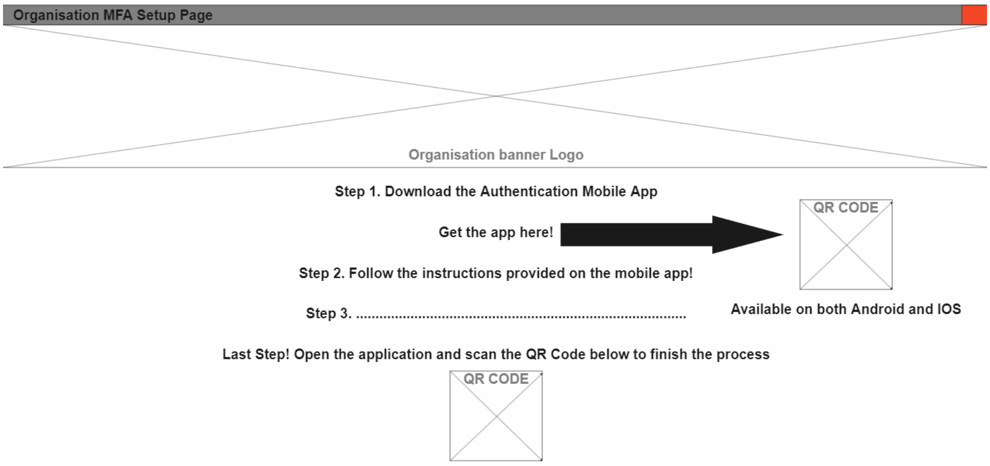
Confirm Password:

Register

Password Policy:
Must be 14 characters or longer
Must include at least one number, uppercase letter, lowercase letter, and special character
Do not share this password with anyone.

Figure 2 Registration Page

Once the employees have successfully signed up or logged in, they would be brought to a page detailing how to set up the required MFA, as shown in Figure 3. To speed up the MFA setup process, QR codes can be integrated as a link to download the mobile application they require for MFA. This ensures the process of signing up is hassle-free for the employees.



Organisation MFA Setup Page

Organisation banner Logo

Step 1. Download the Authentication Mobile App

Get the app here!

QR CODE

Step 2. Follow the instructions provided on the mobile app!

Step 3. ………………………………………………………………………………

Available on both Android and IOS

Last Step! Open the application and scan the QR Code below to finish the process

QR CODE

Figure 3 MFA setup page

Figure 4 is a login page that appears after the MFA has been successfully setup. The login page is completed by entering their previously made or already existing credentials. The forgotten password option has been included as forgetting a password is a common error made by users. MFA can be used alongside their email to confirm the account password is being reset by the employee who created the account.

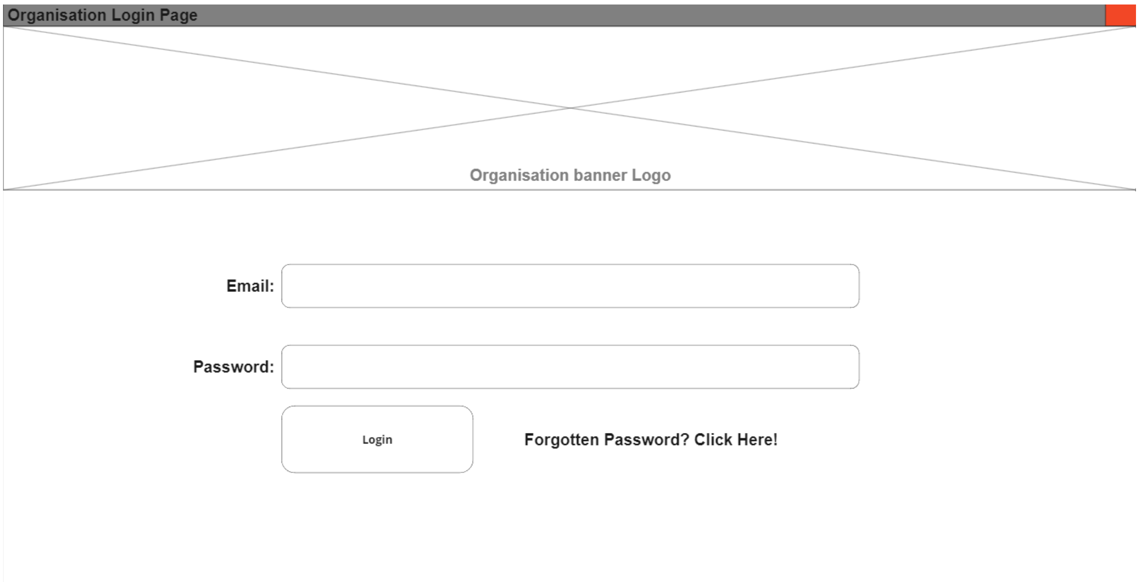
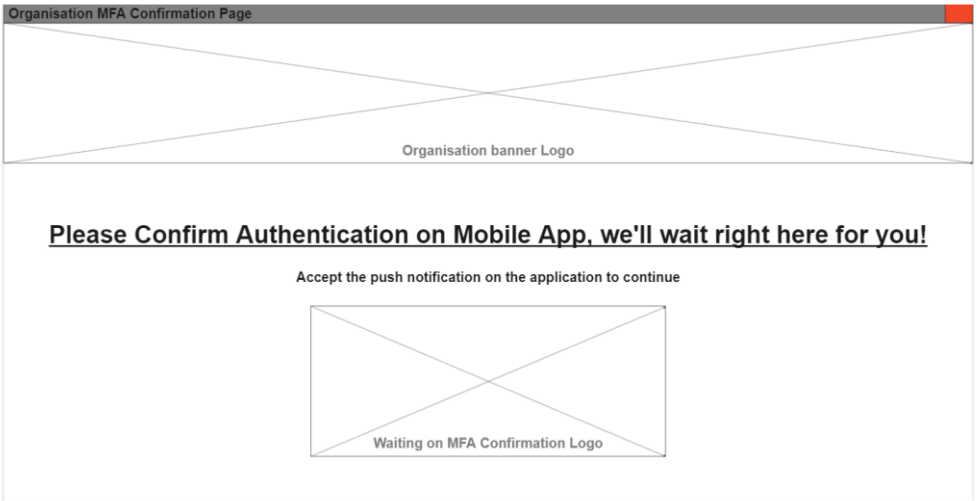


Figure 4 Login page

Figure 5 is the page an employee will see during the MFA process. The webpage will provide concise and clear instructions on how to accept the request that appears on their smartphone. When the request is accepted, they are taken onto the internal web application they wish to access.

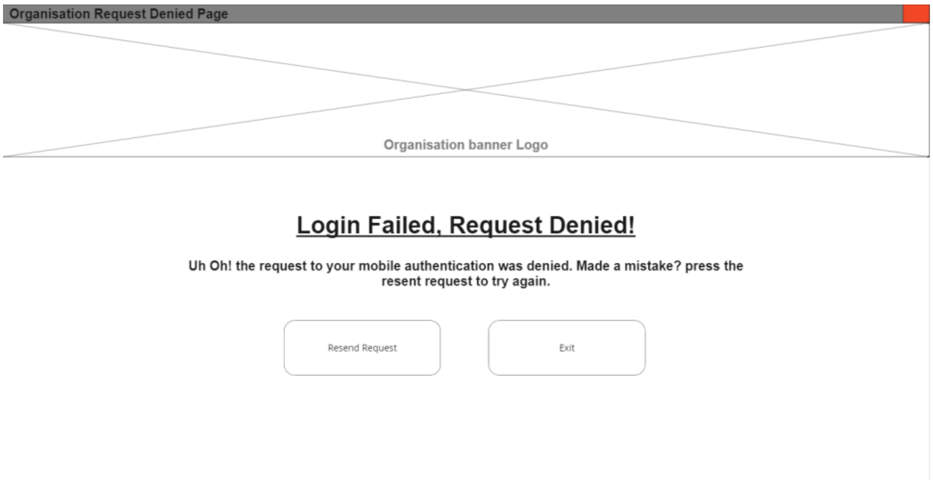

Organisation MFA Confirmation Page
Organisation banner Logo
Waiting on MFA Confirmation Logo

Please Confirm Authentication on Mobile App, we'll wait right here for you!

Accept the push notification on the application to continue

Figure 5 MFA confirmation waiting page

In Figure 6, a page is displayed to users that deny the MFA during the authentication process. An option to resend the request is available, as users are prone to making a mistake and accidentally clicking the deny request button.



Login Failed, Request Denied!

Uh Oh! the request to your mobile authentication was denied. Made a mistake? press the resent request to try again.

Figure 6 Failed Authentication page

Currently, there is no authentication on the internal web application. Scottish Glen should implement the login system using email and password immediately and slowly roll out mandatory MFA while it is being developed. This would provide a basic level of protection against potential threats until MFA is completely integrated into the system.

6 References

Alabdan, R., 2020. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet,* 12(10), p. 168.

Alkhalil, Z., Hewage, C., Nawaf, L. & Khan, I., 2021. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science,* Volume 3.

Alsharnouby, M., Alaca, F. & Chiasson, S., 2015. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies,* Volume 82, pp. 29-82.

Banu, M. & Banu, S., 2013. A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies,* 4(6), pp. 783-786.

Bhanderi, D. et al., 2023. *Impact of Two-Factor Authentication on User Convenience and Security,* New Delhi: IEEE.

Bhavsar, V., Kadlak, A. & Sharma, S., 2018. Study on Phishing Attacks. *International Journal of Computer Applications,* 182(33), pp. 27-29.

Cisco, 2023. *Duo: Next-Level MFA.* [Online]
Available at: https://duo.com/why-duo/next-level-mfa
[Accessed 29 March 2024].

Dasgupta, D., Roy, A. & Nag, A., 2017. *Advances in user authentication.* Cham: Springer International Publishing.

Hadlington, L., 2018. Employees Attitude towards Cyber Security. *International Journal of Cyber Criminology,* 12(1), pp. 269-281.

Jayatilaka, A., Gamagedara, N. A. & Babar, M. A., 2021. *Falling for Phishing: An Empirical,* Austin: Forty-Second International Conference on Information Systems.

Ken Reese, T. S. J. D. J. A. J. C. K. S., 2019. *A Usability Study of Five Two-Factor,* Santa Clara: Proceedings of the Fifteenth Symposium on Usable Privacy and Security.

Kumaraguru, P., 2009. *PhishGuru: A System for Educating Users about,* Pittsburgh: Carnegie Mellon University ProQuest Dissertations Publishing.

Matyáš, V. & Říha, Z., 2002. *Biometric authentication: security and usability,* Portorož: Springer International Publishing.

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

Renaud, K., Volkamer, M. & Maguire, J., 2014. *ACCESS: Describing and Contrasting,* Cham: Springer International Publishing.

Sharma, T. & Bashir, M., 2020. *An Analysis of Phishing Emails and How the Human Vulnerabilities are Exploited.* USA, Springer International Publishing, pp. 49-55.

Sheng, S. et al., 2010. *Who Falls for Phish? A Demographic Analysis of Phishing.* Atlanta, Proceedings of the SIGCHI conference on human factors in computing systems.

Sumner, A. & Yuan, X., 2019. *Mitigating Phishing Attacks: An Overview,* Kennesaw: ACM Southeast Conference.