Abertay University

CMP417 – Engineering Resilient Systems – Human-Centred-Security

Finlay Reid
1904629

Contents

Human-Centred Risks

Phishing or a phishing attack is a form of social engineering in which malicious users attempt to steal critical user data, often through the impersonation of a trusted source such as an email, instant message, or text message. In this particular case, the source of the phishing attacks was email. According to a report conducted by Symantec, there was a steady decline in phishing attacks in 2019; however, within the first quarter of 2020, there was a substantial rise, as phishing emails accounted for 1 in every 4,200 emails (Threat Landscape Trends – Q1 2020, 2020). Furthermore, not only is phishing a popular type of attack, but it is also an effective one, as evidenced by a threat trends report conducted by cisco, which suggests that at least one person clicked a phishing link in around 86% of organisations. The report also indicates that phishing is responsible for about 90% of data breaches (Cybersecurity threat trends: phishing, crypto top the list - Cisco Umbrella, 2021). Users' susceptibility to these attacks can be attributed to many causes, including the sophistication attackers employ to con unsuspecting victims. In addition, criminals exploit technology utilised for spam, distributed denial of service (DDoS), and electronic surveillance to combat users' increasing vigilance against these attacks (Milletary, 2005).

Many papers conclude that one of the main reasons phishing attacks are so effective and can compromise security is some users' lack of technical knowledge. A study conducted by researchers at Carnegie Mellon University in which 232 users participated in several role-play activities found precisely that. The findings suggest that those who rightly answered the knowledge question about the meaning of phishing were notably less likely to fall for phishing emails. Furthermore, the study also showed evidence of lower susceptibility to phishing attacks when the participant better knew web environments. A limitation of the study relates to the sample of participants. All were university members and either had signed up for a survey about online security or had previous abuses of university computer rules. These factors suggest that the users tested are more technologically switched on than the average user (Downs, Holbrook and Cranor, n.d.).

Some researchers refute these claims that a lack of technical expertise indicates increased susceptibility to phishing attacks. In the paper, an integrated information processing model of phishing susceptibility was developed; the model was then applied to a sample of real-world victims of a series of phishing attacks. The results from the experiment showed that technologically savvy users are just as likely to fall for phishing attacks. The paper suggests that a lack of cognitive action is responsible for users' susceptibility to phishing attacks rather than the lack of technical knowledge. A limitation of this study concerns the limited variety of emails tested; the emails tested contained the same information and were of the same quality (Vishwanath et al., 2011).

A real-world example of how phishing attacks can compromise security occurred on the 18th of February, 2005. The attacker sent a large number of emails to thousands of Internet users. The email asked for verfication of their details and confirms that the bank has recently upgraded to a new security system, suggesting that the user confirm the account. In addition, utilising a spoofed webpage masquerading as a legitimate site helps the attack achieve its aims of stealing sensitive data such as the victim's account credentials, credit card information, and personal information. In the context of the risk, this poses to an organisation, company details could also be stolen. This stolen information could be leveraged to do malicious deeds, including leaking critical data, disrupting services or selling the data to the highest bidder (Kirda and Kruegel, n.d.).

The NCSC recommends implementing layers of defence to help organisations defend against phishing attacks. A real-world example outlines that 1800 emails were sent to a financial sector company, but 1750 of these emails were successfully denied by the filtered email service. Fifty emails reached the employee’s inboxes, bypassing the security measures in place, suggesting that there must be security thinking applied to the users themselves to distinguish between phishing emails and non-phishing emails (Phishing attacks: defending your organisation, 2018). The most recent Jisc cyber impact report paints phishing attacks as one of the most effective attacks against companies. It describes them as posing the most significant risk against a company’s employees. The report cites universities as one of the most prominent organisations at risk of phishing attacks, implying that an education mini-course on phishing should be mandatory for students to combat the increasing risk posed by these attacks (jisc, 2022).

Human-Centred Recommendations

As phishing attacks exploit human naivety, there is no one method of mitigating these attacks; instead, a defence in depth approach is recommended. Ensuring employees are educated about phishing is recommended so they can correctly discern between legitimate and phishing emails and then follow the proper procedure should they discover an attack. A limitation of this method involves the resistance to learning some non-technical users may have, and there is no guarantee that users will retain this knowledge(Khonji, M., Iraqi, Y. and Jones, A., 2013). As previously mentioned, this line of thought that user education mitigates phishing attacks has been questioned by many researchers(Gorling, S., 2006).

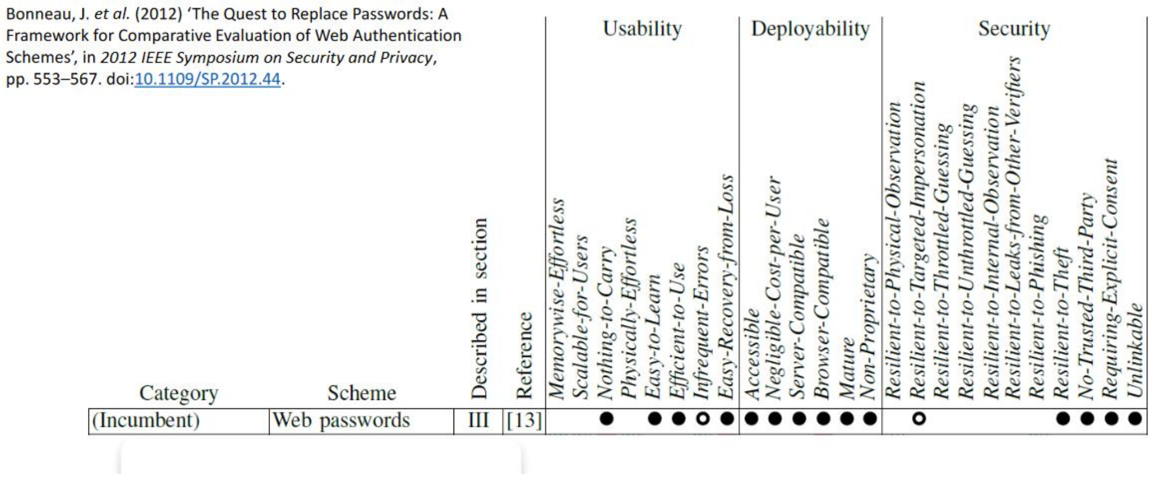
A recommended solution to mitigate phishing attacks exists on the end of the software developer. Increasing the usability of systems through the improvement of user interfaces can ensure that users devote full attention when prompted with a vital system message. In the past, security messages have utilised passive warnings ensuring users fail to read the warnings. However, recent web browsers have implemented active warnings that convey the risks without user understanding(Khonji, M., Iraqi, Y. and Jones, A., 2013).

An unusual human-centred approach to mitigating the risk posed by phishing attacks involves applying mindfulness techniques to dynamically allocate attention during message evaluation, improve understanding of context, and forestall judgment of suspicious messages. Again this method does not reduce phishing attacks to zero but is effective as part of a larger mitigation plan that complements other techniques. A study of 1048 faculty, staff, and students who participated in a study demonstrated the efficacy of this technique, reporting a high level of expertise in identifying phishing emails. A drawback of this mitigation technique involves the length that employees/users would retain the knowledge of mindfulness(Jensen et al., 2017).

Authentication Mechanisms

Passwords have been the preferred authentication mechanism even before the advent of computers, but they have many limitations, and users become lazy, utilising the same password over multiple accounts. Furthermore, users commonly include vital words related to their life, namely hobbies or interests in their password so they are easily remembered. This makes a malicious user's life much simpler when attempting to gain unauthorised access to a company account or personal information. For example, a 2016 report conducted by Verizon determined that 63 % of verified data breaches involved weak, default or stolen passwords(Ford, 2022). The results suggest that using a single password to secure a user's account is an inadequate authentication method. As a result, security practitioners have developed new authentication methods to mitigate the drawbacks of single passwords. Security practitioners have attempted to improve the effectiveness of password authentication and mitigate the weaknesses by implementing password policies. Often enforcing users on sign up to include specific characters and meet a required length. Several studies have investigated the supposed increase in security that password policies grant. Including a study undertaken by researchers that tested the crackability of passwords with the trade-off in usability through two carefully prepared experiments. The results demonstrated that passwords produced with a more rigorous form of guidelines were more resistant to automated cracking but substantially more onerous to invent and then later remember(PROCTOR et al., 2002).

In order to successfully evaluate authentication schemes, numerous methods have been constructed and published in papers, including by researchers at the University of Cambridge. This paper presents an evaluation model covering three categories: usability, deployability and security. Within each of these categories is a benefit with a provided definition, as shown in **Figure 1**; if the authentication method meets the criteria for that benefit, it achieves a pass for that specific metric. This framework provides a good list of predefined definitions that were consistently refined, allowing for the comparison to the authentication model being tested. Furthermore, It covers a vast number of benefits (Bonneau, Herley, van Oorschot and Stajano, 2012). Another paper that presents a method for evaluating authentication procedures includes the paper produced by researchers at San Jose University. The aforementioned paper approaches the evaluation in a human-centred manner, outlining a list of human-centred authentication problems into an inventory of practical guidelines. Six in-depth guidelines are included, including designing the authentication interface inclusive, considering accessibility and usability. However, a limitation of the paper is the failure to include any examples of the guidelines applied to authentication schemes. Furthermore, a drawback of the evaluation model includes the focus on one criterion, the human element(Still, J.D., Cain, A. and Schuster, D., 2017).



Bonneau, J. *et al.* (2012) 'The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes', in *2012 IEEE Symposium on Security and Privacy*, pp. 553–567. doi:10.1109/SP.2012.44.

				Usability								Deployability						Security										
Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●

Figure 1 – Evaluation Model Benefits Checklist

Authentication schemes fall into three distinct types what you know, what you hold and what you are. What you know types involve a knowledge-based model, including but not limited to a basic password, PIN code, or a lock pattern. On the other hand, what you hold type is something the users possess, a possession factor that could be or utilise a cell phone, RFID and a smart card. Finally, what you are authenticating relies on an inheritance factor, typically a fingerprint, iris and palm-based authentication method(Zviran, M. and Erlich, Z., 2006). Each of these authentication types is susceptible to varying attacks and has drawbacks. For example, the authentication schemes that utilise a knowledge-based approach are vulnerable to keylogging, brute force and guessing attacks (Barkadehi et al., 2018). When selecting the appropriate authentication scheme, it helps to take the viewpoint of how much assurance is required, thus allowing a decision to be made on the level of verification. Considering these two metrics, the context of the issue and evaluation results utilising a model such as the one shown in **Figure 1** helps make a final decision regarding an authentication scheme.

In order to provide additional security to the process of authentication, a method was developed that factored in two types of authentication known as two factor. It functions by having a user present two pieces of evidence. For example, the user would be queried for their password; if successful, a one-time passcode would be sent to their device for further verification. Therefore two factors are authenticated, what they know in the case of the password and what they hold for the one-time passcode. Including this additional layer of security ensures that should a malicious attacker possess a user's password through whatever means, they will not be able to access the organisation without the one-time passcode. Furthermore, one time codes have expiration implemented to mitigate the risk posed by brute force attacks(Schneier, B., 2005).

Authentication Recommendations

Multifactor authentication requires users to present two or more types of evidence, meaning all 2FA is an MFA, but not all MFA is a 2FA. Multifactor authentication is simple to set up and typically involves scanning a QR code, inputting relevant data such as a phone number or downloading a specific app such as Microsoft authenticator. These mechanisms can be highly effective if implemented correctly; as previously mentioned, a malicious user would require access to the device and have the password. Furthermore, most systems today implement a notification feature that pings the user if a new location or device has been utilised to log in.

In the context of the company's internal web applications, implementing multi-factor authentication would significantly decrease the risk of attackers gaining access to the company's systems. Selected due to the high level of confidence and stringent verification required as the company restricted data would be accessible if authentication measures are bypassed. As described in the assessment brief, there is a limited budget with a small development team, so implementing several inherence-based schemes is ruled out, including palm print biometrics, hand gestures and face biometrics. The simplicity of two-factor authentication helps negate the risk of employees not understanding specific authentication mechanisms. This, combined with application-based authentication and email-based should the employee not own a phone, ensures the system covers every demographic. If the application and email cover the possession type of authentication, the knowledge type would be covered by a password that implements a firm password policy involving over sixteen characters. This is known as the most robust protection against brute force attacks. Finally, both of these selected authentication schemes scored well in the model shown in **Figure 1**.

Several critical decisions were made and considered to maximise usability and accessibility. One example is that on every authentication interface, there is a title to remind the user what they are doing. All interfaces utilise the bold, clear font to ensure users can easily discern what should be inputted and could assist any users with impaired vision. Furthermore, all interfaces are simple, allowing users to follow what is required quickly. In **Figure 3**, the cancel button is shaded in the colour red to convey that a button press will cancel the login attempt.

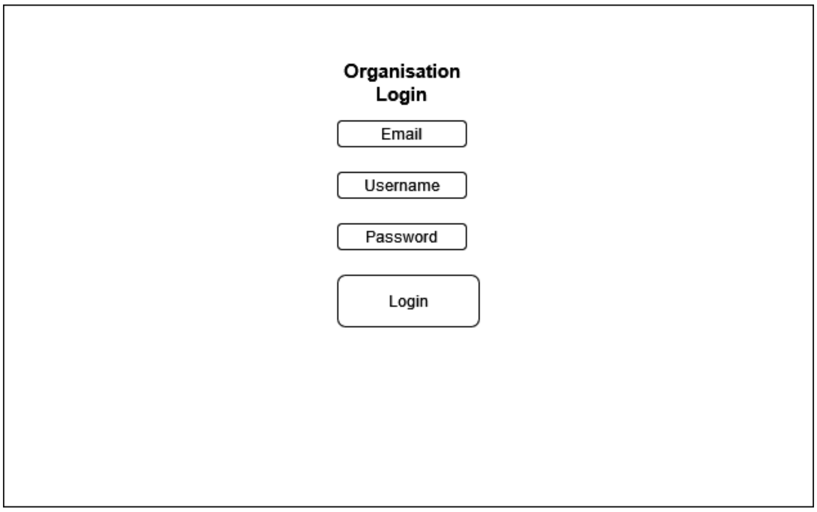


Figure 2 - Company Login Page Authentication Design

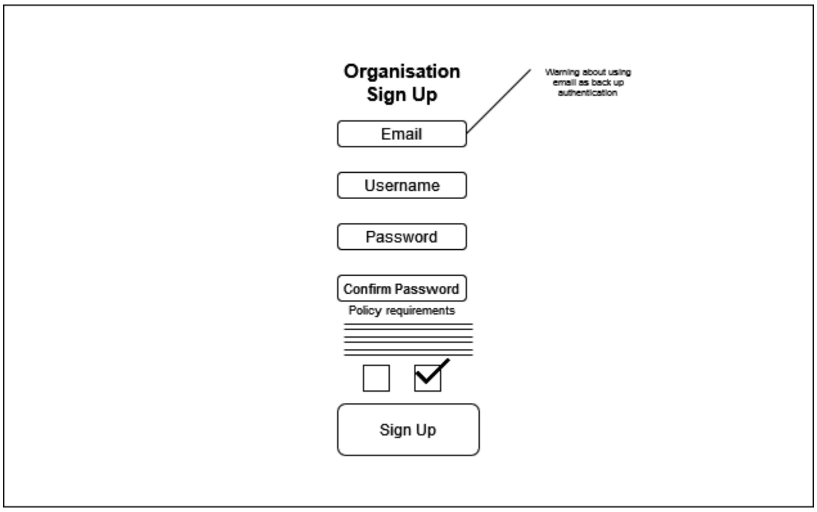


Figure 3 - Company Sign Up Page Authentication Design

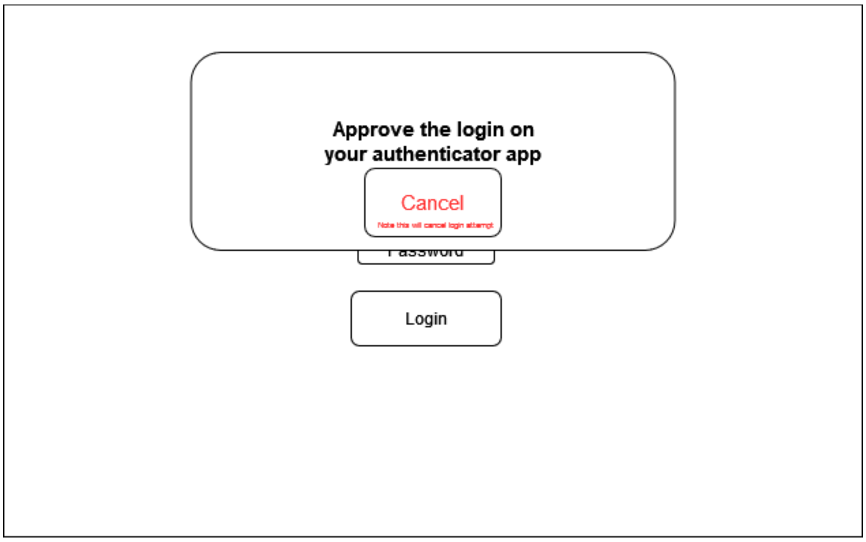

Approve the login on your authenticator app
Cancel
Note this will cancel login attempt
Password
Login

Figure 4 - Company Pop Up Warning For Authentication Design

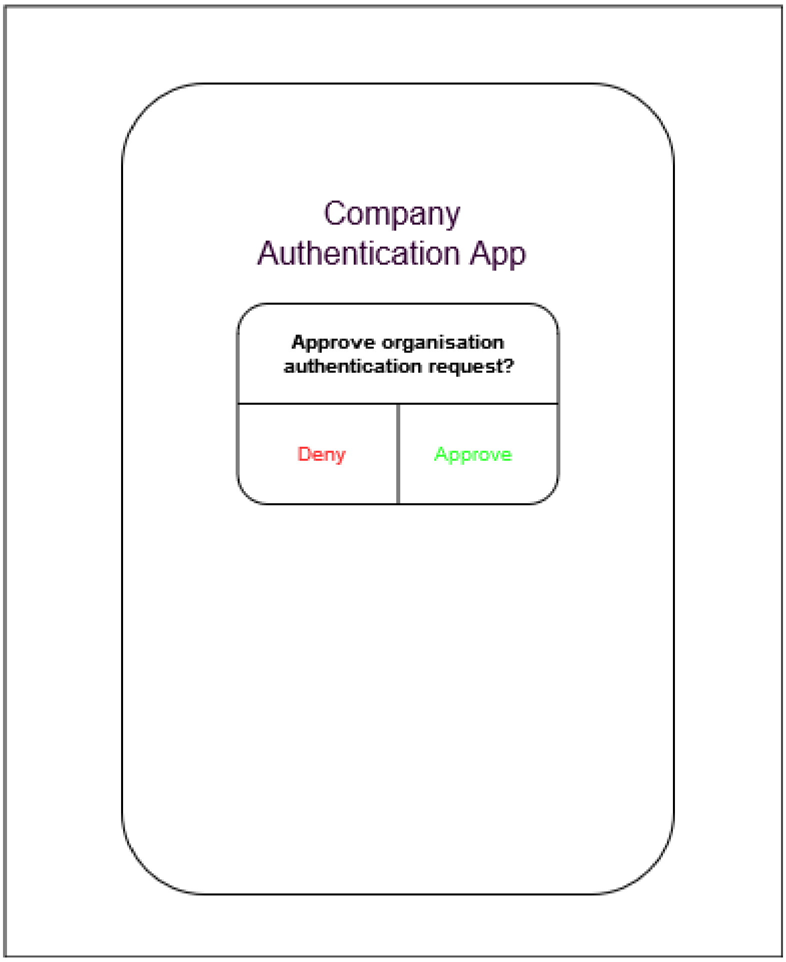


Figure 5 - Company App Pop Up Approval Message Design

References

Barkadehi, M.H., Nilashi, M., Ibrahim, O., Fardi, A.Z. and Samad, S., 2018. Authentication systems: A literature review and classification. Telematics and Informatics, 35(5), pp.1491-1511.

Bonneau, J., Herley, C., van Oorschot, P. and Stajano, F., 2012. The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes. [online] Cl.cam.ac.uk. Available at: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf> [Accessed 22 May 2022].

Cisco Umbrella. 2021. Cybersecurity threat trends: phishing, crypto top the list - Cisco Umbrella. [online] Available at: <https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list> [Accessed 20 May 2022].

Downs, J., Holbrook, M. and Cranor, L., n.d. Shibboleth Authentication Request. [online] Dl-acm-org.libproxy.abertay.ac.uk. Available at: <https://dl-acm-org.libproxy.abertay.ac.uk/doi/pdf/10.1145/1299015.1299019> [Accessed 20 May 2022].

Ford, N., 2022. 63% of data breaches involve weak, default or stolen passwords - IT Governance UK Blog. [online] IT Governance UK Blog. Available at: <https://www.itgovernance.co.uk/blog/63-of-data-breaches-involve-weak-default-or-stolen-passwords> [Accessed 22 May 2022].

Gorling, S., 2006, October. The myth of user education. In Proceedings of the 16th Virus Bulletin International Conference (pp. 11-13).

Jensen, M.L., Dinger, M., Wright, R.T. and Thatcher, J.B., 2017. Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems, 34(2), pp.597-626.

jisc, 2022. Cyber Impact 2020. cyber impact. [online] jisc. Available at: <https://repository.jisc.ac.uk/8732/1/cyber-impact-report-2022.pdf> [Accessed 21 May 2022].

Kirda, E. and Kruegel, C., n.d. Protecting users against phishing attacks with AntiPhish. [online] Ieeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/abstract/document/1510078> [Accessed 21 May 2022].

Khonji, M., Iraqi, Y. and Jones, A., 2013. Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials, 15(4), pp.2091-2121.

Milletary, J., 2005. [online] Ftp.unpad.ac.id. Available at: <http://ftp.unpad.ac.id/orari/library/library-ref-eng/ref-eng-3/network/network-security/cert/techtips/Phishing_trends.pdf> [Accessed 20 May 2022].

NCSC. 2018. Phishing attacks: defending your organisation. [online] Available at: <https://www.ncsc.gov.uk/guidance/phishing> [Accessed 21 May 2022].

PROCTOR, R., LIEN, M., VU, K. and SCHULTZ, E., 2002. Improving computer security for authentication of users: Influence of proactive password restrictions. [online] Link.springer.com. Available at: <https://link.springer.com/content/pdf/10.3758/BF03195438.pdf> [Accessed 23 May 2022].

Schneier, B., 2005. Two-factor authentication: too little, too late. Communications of the ACM, 48(4), p.136.

Still, J.D., Cain, A. and Schuster, D., 2017. Human-centered authentication guidelines. Information & Computer Security.

Symantec-enterprise-blogs.security.com. 2020. Threat Landscape Trends – Q1 2020. [online] Available at: <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020> [Accessed 19 May 2022].

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H., 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model.

Zviran, M. and Erlich, Z., 2006. Identification and authentication: technology and implementation issues. Communications of the Association for Information Systems, 17(1), p.4.