Abertay University

Human-Centred Security

Jordan Gribben

CMP417: Engineering Resilient Systems Part 3

BSc Ethical Hacking Year 4

2021/22

1 PHISHING

1.1 HUMAN-CENTRED RISKS

Phishing attacks typically take the form of an email or message, these messages are designed to exploit a moment of vulnerability within the recipient be it; curiosity, fear, or empathy (Chaudhry, et al., 2016). This vulnerability is exploited with a fake scenario prompting a user to complete a task either in the real world or online, e.g, downloading a file, logging into a fake website, purchasing gift cards. The exploitation of a human weakness can stop many from thinking logically. Every person comes from a unique background with countless events going on at a given moment. Phishing prays on this human element, causing some to be more susceptible to these attacks than others (Alkhalil, et al., 2021). The most common triggers for people are curiosity and urgency, with these being the leading cause of why phishing attacks are successful (PhishMe, 2017). Additionally, authority plays a key role in falling victim to phishing. When the source of a phishing message comes from someone pretending to be an authority figure, like a departments boss, or company CEO, it becomes more likely that someone will fall victim to the attack (JoanneHinds & N.Joinson, 2018).

This leads to phishing being the top method of exploitation within businesses. 41% of incidents against businesses during 2021 were caused due to a phishing attack, these attacks provided malicious users initial access to further compromise a system (IBM, 2022). At 41% smaller businesses may think they are unlikely to be targeted, this however is untrue, with around 58% of small businesses facing cyber attacks (Bikov, et al., 2019).

There are many indicators that can be used to identify phishing attacks. Due to phishing exploiting a weakness found in humans rather than a technical exploit, training users to spot these indicators is the first step in mitigating against phishing (Salem, et al., 2010). The National Cyber Security Centre provide various cyber security guides, one of their guides details common signs of phishing that people should look out for. These signs include; poor spelling/grammar, poor quality images, high ranking people, asks you to act urgently, how the email addresses you, and if it sounds too good to be true (NCSC, 2017). People that remain uninformed or ignorant of these signs are likely to end up victims to phishing due to their own irresponsibility.

While for the trained eye phishing attempts can be seen as obvious, the scammers will use any tactic they can to ensure their attacks are successful. During the COVID-19 pandemic many scammers saw this as an opportunity to phish for victims. Scam messages with links/downloads related to COVID-19 prayed on peoples need for urgency, with these links/downloads promising, important covid updates, Personal Protective Equipment (PPE) orders, government pay-outs, and track and trace notifications (NCSC, 2020). Within the UK the number of COVID-19 related attacks peaked around the start of the pandemic, with these attacks spiking in popularity after the UK's first confirmed COVID-19 related death, further playing on peoples fear and urgency (Microsoft 365 Defender Threat Intelligence Team, 2020). Scammers trying to take advantage of COVID-19 often used authority figures to further sell their scams, by pretending to be, an official government body/system (e.g, NHS, Track & trace, UK Gov), a doctor, or a reliable seller. By combining the two key triggers of authority and urgency (brought on by the pandemic and need for resources) it is clear why these scams were so popular and why so many fell victim.

This information shows that if employees are uninformed of current phishing scams, untrained in ways to detect phishing, and play into their emotions, they are likely to fall victim to phishing.

1.2 HUMAN-CENTRED RECOMMENDATIONS

ScottishGlen employees will receive mandatory training to improve their resilience against phishing. This training will involve 3 key topics based off the literature reviewed in the previous section:

- Human emotions
- Common phishing signs
- Current scams

Focusing on human emotion, employees will be informed about the emotions phishing attacks tend to pray on. While it is impossible to control how someone feels, or their personal circumstances when a phishing attempt is received, by explaining that these attacks pray on human emotions and work when we are at our weakest it could help prevent a successful phishing attempt. Employees will be told to take a step back, double check any communications to ensure they aren't phishing. If they are still unsure, get a co-worker to check, if the email has come from an authority figure email them directly asking if this is real. Teaching the common elements phishing tends to pray on will lead staff to be more wary when a message engaging in these triggers is received.

Common phishing signs will be discussed with staff, explaining what to look out for within communications. Employees should double check email addresses especially ones pretending to be authority figures, this will help mitigate various phishing attempts. The contents of phishing messages should also be examined, looking for key signs such as poor grammar and poor-quality images. Employees will be taught on how to properly read a URL as it is common for the domain to be incorrect in phishing emails. In addition to being taught how to read a URL the main advice given to employees at this stage would be to access all sites directly instead of via a link in an email, doing this will prevent any bad URL's from being clicked.

Employees will be kept up to date with current scams, if employees notice any new trending scams, they should inform the appropriate authority figure immediately. A notification will then be sent out detailing what this phishing scam is looking for. This will be crucial at avoiding phishing attacks, especially during times were ScottishGlen may need to act with urgency, such as purchasing PPE.

Phishing attacks can also lead its victims to a fake website prompting them to input their login credentials. It is recommended that authentication mechanisms are in place to ensure the account is not fully compromised.

2 AUTHENTICATION

2.1 INTRODUCTION

When it comes to authentication there are 3 main types:

- What you know – This method uses information only a user knows to authenticate them. This is commonly seen in the form of a password.
- What you have – This method uses information using something a user possess, this could take the form of a one-time code or key.
- What you are – This method uses information about the user for authentication. This is commonly seen with biometrics, using fingerprint/iris scanners.

Each type of authentication is unique compared to each other despite them all achieving the same goal (Lal, et al., 2016). Each type has its advantages and disadvantages alongside accessibility features/concerns. Authentication mechanisms for each type will be reviewed and discussed before implementation within ScottishGlen.

2.2 AUTHENTICATION MECHANISMS

The most common form of authentication is the password, a password is a "what you know" type of authentication. A strong password does not come from complex password policies, these policies tend to annoy users to the point where they create passwords that just meet the requirements, this tends to make the passwords easy to guess leaving them as insecure (Christmann, et al., 2021). These policies also give malicious users a good idea on what a password needs making them easier to brute force, this is especially true if a maximum character limit is in place. Strong passwords are great form of authentication making it hard for attackers to crack/guess. However, they can also be difficult for users to remember (Dell'Amico, et al., 2010), this ultimately causes the passwords biggest downfall. Due to them being the most common used method of authentication users cannot remember hundreds of strong passwords and revert to weaker passwords or repeating the same password. To prevent against this a tool such as a password manger could be used. However, the memorability of the password is not directly linked to the password's length (Jain, 2018). A 16-character password could take up to 6.5 trillion years to brute force (Kast, 2020), if users want stronger accessible/usable passwords, they could make them longer rather than fit absurd password policies.

A "what you have" authentication method is Multifactor Authentication (MFA)/2 Factor Authentication (2FA). MFA/2FA forces a simple check once a user has successfully logged in, typically prompting them to input a code from their email or MFA application. By adding 2FA accounts will become more difficult to break into, in turn help protect sensitive information that may be accessed from these accounts. This technology can be seen as easy to use (Jessica Colnago, 2018) and can be easily enforced within ScottishGlen. Previous research into MFA details that when this technology is forced on users there is no significant change in experience/impact compared to those that use it by choice (Abbott & Patil, 2020). This research also indicated that 2FA was annoying when it was used continuously.

For "what you are" biometrics are by far the most popular. Modern smartphones commonly pair both biometrics alongside passcodes as their methods of authentication. Fingerprint sensors are by far the

most popular form of biometric authentication, they are extremely common in mobile devices with 60% of smartphones shipped in 2018 containing a fingerprint sensor (O'Dea, 2020). Apple devices use capacitive sensors for their fingerprint sensors, these are extremely difficult to spoof due to a finger being used as a conductor to complete the circuit, with each fingerprint having unique ridges and patterns the resistance from different fingers will be unique (Dongdong, 2017). Facial recognition is another key feature found on modern smartphones, this uses the front facing camera to authenticate the user. This technology uses complex algorithms to map out and identify faces, some of these algorithms seek out key facial feature like the size/shape of a nose (Park, et al., 2014).

2.3 AUTHENTICATION RECOMMENDATIONS

For ScottishGlen it is recommended a mixture of all 3 authentication types are used for maximum security. While complex this can be done with both accessibility and useability in mind, keeping the system inclusive. A wireframe version of the proposed system can be seen in figure A.

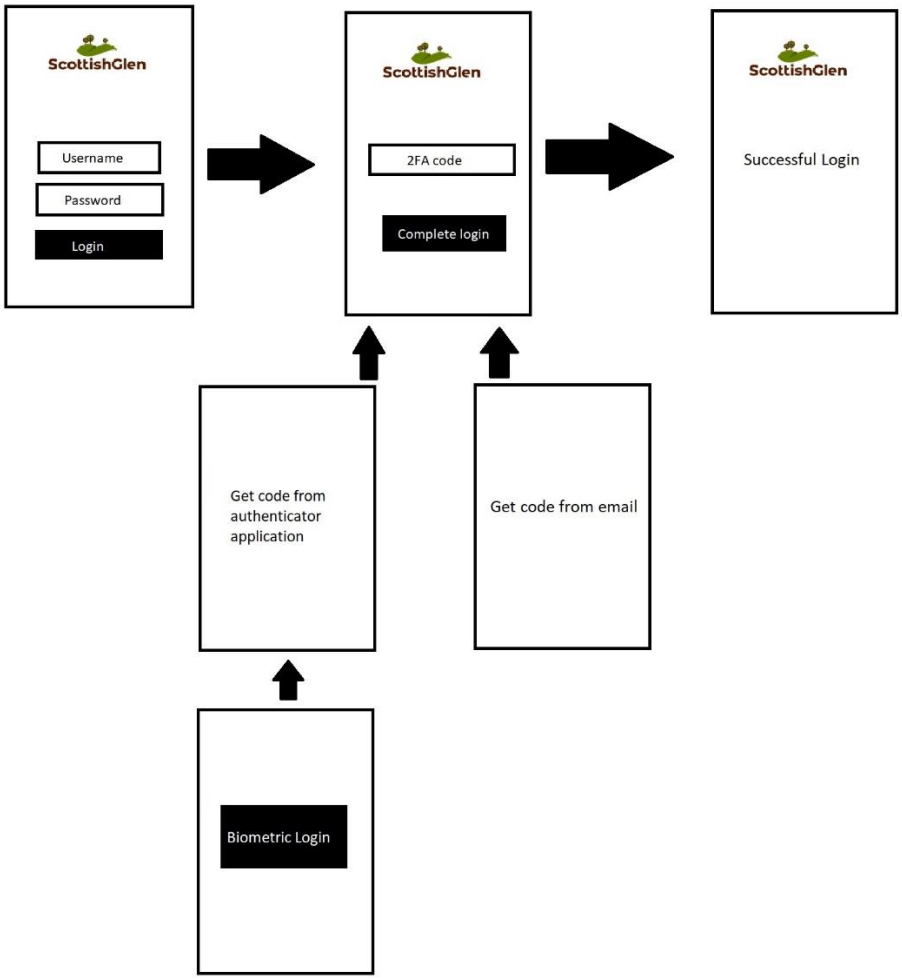

Figure A - Wireframe authentication system

A strong password policy will be implemented within ScottishGlen requiring over 16 characters. While strong passwords are impersonal for accessibility/usability purposes this rule will not recommended, instead staff should use something from their lives only they know like

“TheNumber4BusIsAlwaysRunningLate”. This will allow staff to create a strong memorable password without it being something obvious.

After a user has logged in, they will be prompted to enter a code using 2FA. 2FA will be enforced on all users as enforcing this authentication technique has little impact. All staff will receive 8 backup codes further adding to the tool’s accessibility. These codes can be used in the event staff cannot access their 2FA and need in their system, these backup codes are one time use. ScottishGlen employees will be given 2 options for 2FA:

- Email – This will be the default method of 2FA enforced on staff. Staff will receive a code via email after login, this code must be input before the login can be complete.
- Authentication App – This method will not be enforced but strongly recommended to staff, the benefits of using an authentication application will be explained to staff so they are more likely to use it. The Microsoft authenticator application will be the chosen application for ScottishGlen. The app can be downloaded onto a user’s smartphone, the app contains codes that expire after a set time, once expired a new code is set. A user must input this code to complete the login process.

The “what you are” method of authentication will be implemented alongside the authentication app. Microsoft authenticator allows users to use their smartphones biometrics to sign into the application, this adds a further layer of security for those using the app as if their account were to be compromised and smartphone stolen the malicious user would still not be able to access the codes to gain access to the account. For staff using the app, they will be encouraged to set up the biometric sign in if their device is compatible.

This authentication system has been created with usability and accessibility in mind. The password system allows from strong and memorable passwords to be made, without too many requirements for users to remember keeping it usable. Having the choice of multiple 2FA methods allows employees to pick the one they feel most comfortable with. Email 2FA as the default is good for accessibility as it does not discriminate against employees for the devices they own, the authenticator application may not work with older devices and forcing employees to upgrade their device just for an authentication method could be seen as unethical. Additionally, not requiring the use of biometrics with this application further demonstrates this viewpoint. To maintain usability for this authentication system ScottishGlens web application should be a single sign on system to prevent users from becoming frustrated at constantly entering passwords/2FA codes.

3 REFERENCES

Abbott, J. & Patil, S., 2020. *How Mandatory Second Factor Affects the Authentication User Experience.* New York, Association for Computing Machinery.

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

Bikov, T. D., T. B. I., Mihaylov, G. Y. & Stoyanov, I. S., 2019. *Phishing in Depth – Modern Methods of,* Opatija: IEEE.

Chaudhry, J. A., Chaudhry, S. A. & Rittenhouse, R. G., 2016. *Phishing Attacks and Defenses,* Innopolis: International Journal of Security and Its Applications.

Christmann, M., Mayer, P. & Volkamer, M., 2021. *How to Effectively Communicate Benefits of Introducing a Modern Password,* Karlsruhe: Karlsruhe Institute of Technology.

Dell'Amico, M., Michiardi, P. & Roudier, Y., 2010. *Password Strength: An Empirical Analysis,* Sophia Antipolis: IEEE.

Dongdong, W., 2017. *Introduction of capacitive fingerprint sensor,* Beijing: Institute of microelectronics, Tsinghua University.

IBM, 2022. *X-Force Threat Intelligence Index,* New York: IBM.

Jain, A., 2018. *Review of Password Security,* Jagdishpur: Mahavir Swami Institute of Technology.

Jessica Colnago, S. D. M. O. C. S. L. B. L. C. C., 2018. *"It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University.* New York, ACM Digital Library.

JoanneHinds, E. J. & N.Joinson, A., 2018. *Exploring susceptibility to phishing in the workplace,* Bristol: International Journal of Human-Computer Studies.

Kast, B., 2020. *How long should your password be? The data behind a safe password length policy.* [Online]
Available at: https://www.lmgsecurity.com/how-long-should-your-password-be-a-technical-guide-to-a-safe-password-length-policy/
[Accessed 21 May 22].

Lal, N. A., Prasad, S. & Farik, M., 2016. *A Review Of Authentication Methods,* Chicago: INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME.

Microsoft 365 Defender Threat Intelligence Team, 2020. *Exploiting a crisis: How cybercriminals behaved during the outbreak,* London: Microsoft.

NCSC, 2017. *Small Business Guide: Cyber Security.* [Online]
Available at: https://www.ncsc.gov.uk/collection/small-business-guide/avoiding-phishing-attacks
[Accessed 20` May 2022].

NCSC, 2020. *Advisory: COVID-19 exploited by malicious cyber actors,* London: NCSC.

O'Dea, S., 2020. *Share of smartphone shipments with a fingerprint sensor worldwide from 2014 to 2018.* [Online]
Available at: https://www.statista.com/statistics/804269/global-smartphone-fingerprint-sensor-

penetration-rate/
[Accessed 28 October 2021].

Park, Y. Y., Choi, Y. & Lee, K., 2014. *A Study on the Design and Implementation of Facial Recognition,* Asan: Department of Computer Engineering, Sunmoon University, Korea.

PhishMe, 2017. *Enterprise phishing resiliency and defense report,* Leesburg: Cofense.

Salem, O., Hossain, A. & Kamala, M., 2010. *Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks,* Bradford: IEEE.