Part 3 - Human-Centred Security

Patrick Collins
1900609

Contents

Scenario

ScottishGlen is a small company within the energy sector. Employees have been receiving messages from a hacktivist group, who threaten to target the company following a recent blog post by the CEO. It is not known the nature of the attack they are planning. The CEO is concerned and has asked the IT manager to improve the security posture to better protect the company.

Several employees have been receiving phishing emails which look to be from the hacktivist group. It is likely just a matter of time before someone opens a malicious link, or attachment, and exposes the company network. The IT manager was asked to review the situation and recommend a multi-layered set of mitigations or mechanisms to improve the company’s human-centred resilience against phishing attacks.

There is also a concern that some of the company’s internal web applications currently don’t require employees to authenticate themselves. While this is convenient, the company now considers this a risk. There is limited budget to address the situation, but some of the developers can be allocated to create a solution. The IT manager was asked to identify a suitable authentication mechanism, balancing security and usability.

Human-centred risks

A Phishing attack occurs through the employee (End User) receiving a malicious email enticing staff to click a malicious link or download a malicious attachment (NCSC, 2022). As ScottishGlen has come under attack by a hacktivist group this is also a targeted phishing campaign and could lead to spear phishing where the attacker uses legitimate information about the company and its employees to make the malicious email more convincing to the staff to trust the link/download the attachment (NCSC, 2022).

A very informative paper from over a decade ago by Zulfikar Ramzan in 2010 titled "*Phishing Attacks and Countermeasures*" goes over the main countermeasures advised from that time on how to prevent phishing attacks. The main points identified in the literature are (Ramzan, 2010):

- Two-Factor Authentication
- Email Authentication
- Secure Sockets Layer (SSL)
- One-Time Credit Card Numbers
- Back-End Analytics

Two years later further research carried out by Jason Hong in 2012 with their paper titled "*The State of Phishing Attacks*" presents further countermeasures against phishing attacks. This time however focusing on Human-Centred Security against phishing attacks. The main points identified in the literature are:

- Train users against phishing attacks
- Improve User Interfaces
- Two-Factor Authentication
- Email Filtering and blocking phishing sites

We begin to notice a change in countermeasures with educating and training users against the threat of phishing becoming a priority. Advice was now to train the user on how to identify a phishing attack if the email bypasses security measures. User interfaces were advised to be improved using active alerts to engage the user to recognise a phishing attack warning and thus result in less successful phishing attacks. Also, by improving how the user authenticates with the website using Two Factor Authentication (2FA). The final countermeasure concludes that making the phishing attempt invisible to the user in the first place is a good enough prevention as any. It essentially solves the problem at its root. This can be done through Email Filtering and blocking known phishing sites. If the end user does not receive a phishing attack, then there is no risk to the user and the organisation (Hong, 2012).

A more recent investigation into anti-phishing countermeasures was undertaken by Ankit Kumar Jain & B.B. Gupta in 2022 with their research titled "*A survey of phishing attack techniques, defence mechanisms and open research challenges*". Their research highlights what an attacker is aiming to obtain from their phishing attacks. A phishing attack against an organisation attempts to steal the names, social security numbers, addresses, and account information of employee, R&D and product information, financial information, customer credentials with the intention to sell this information (Ankit Kumar Jain & B.B. Gupta, 2022).

The main points identified in this literature are (Ankit Kumar Jain & B.B. Gupta, 2022):

- User education approaches: Phishing avoidance by security warning, Game-based training approaches.
- List-based anti-phishing solutions
- Visual similarity-based techniques

Today, advice is given by the National Cyber Security Centre to companies on how to prevent phishing attacks (NCSC). A real-world example as presented by the NCSC found that Email Filtering had a 97% success rate at stopping a phishing campaign against a company in aims to deploy malware. Out of 1800 phishing emails sent in the targeted attack, 1750 were caught and filtered using Email Filtering (NCSC, 2022). For the emails that bypassed filtering, around half of the Staff who received the phishing email identified them as suspicious and reported them. Training staff on how to identify and respond to phishing emails further protected the company against this targeted attack. Had these measures not been put in place, the attack could have been devastating to the company highlighting the importance of Human-centred Security within organisations.

Human-centred recommendations

As identified in the literature review there are many countermeasures that help prevent a phishing attack on an organisation through the end user. The first recommendation that the IT manager recommends that ScottishGlen implement is Email Filtering due to its proven success at preventing a targeting phishing attack which the company is currently facing by the hacktivists.

Specifically, Defender for Office 365 should be implemented immediately for its extra anti-phishing protection in Exchange Online Protection (EOP) than using the basic EOP (Chrisda et al., 2023). Anti-phishing polices can be created that allow various options such as setting the Phishing email threshold (Standard to Most Aggressive), impersonation prevention and domain protection. The policy allows you to select up to 350 users to protect against impersonation which is perfect for the small business that ScottishGlen is. Furthermore, if the policy triggers an alert the administrators will be immediately notified of the phishing attack (Chrisda et al., 2023).

Configuring Defender for Office365 with these policy features will enable ScottishGlen to set up good email filtering to prevent the targeted phishing attack and impersonation of its staff. This first layer of defences will catch most if not all the phishing emails before it reaches staff’s email inboxes. However, further layers must be implemented to increase the companies resilience even more against a phishing attack.

The second recommendation is to provide effective training to all users against a phishing attack. Educating staff will prove invaluable if the email happens to bypass the email filtering (Gordon et al., 2019). Staff will be able to report the malicious email to ScottishGlen and prevent a malicious attack on the company.

However, it’s very important how this training is undertaken. The training could be performed in a workshop environment by getting staff to craft their own phishing email which will help staff get a better understanding of common techniques used by the attackers (NCSC, 2022). Furthermore, a clear message should be given to the staff that phishing emails can be very difficult to spot and it is ok if one is not caught. The objective is to have understanding and to never punish the user if a phishing attack is successful to encourage the next phishing attempt to be reported (NCSC, 2022).

Whilst these recommendations appear effective it’s also important to consider what impact the new recommendations will have on the staff. For starters, legitimate email may be flagged as malicious email and could disrupt workflow within ScottishGlen. The anti-phishing polices should be reviewed and reconfigured should this happen. Some staff may also need extra support after phishing training to understand the threat better and have more confidence to spot and prevent the attack. Extra support should be available and encouraged for staff should they need it (Gordon et al., 2019)

Authentication mechanisms

A web app without any authentication measures is a massive security risk and an easy target for the hacktivists. Whilst ScottishGlen only use the web apps internally and is not exposed outside the company, this is still a threat if the hackers manage to gain initial access to the internal network.

The essential authentication mechanism for any website is to create a log in system (Velásquez et al., 2018). This can be done by the User creating a Username and Password and supplying it when logging in to the website. The hacktivists will be well versed on this common security measure and the weaknesses that come with it. To ensure the Users are creating secure passwords to mitigate these attacks a password policy should be created which forces the Users to create passwords that meet certain requirements.

The National Cyber Security Centre (NCSC) provides a very thorough guide on password policy creation (NCSC, 2018). Password managers could be used to generate secure passwords instead of the staff trying to create one themselves but are generally more difficult for staff to adopt. If the user attempts to create their own password, then it's likely it will be weak and easily guessable by an attacker. Attempting to implement password complexity checks (by requiring special characters, numbers, upper case etc) also provide no defence and should not be used when making secure passwords (NCSC, 2018, OWASP, 2021).

Instead, it is better to encourage users to create a password using three random words such as "grassempiremoney" (McCormack, 2016). A minimum password length should be enforced although there shouldn't be a maximum password limit. However, an attacker still may get through this first layer of defense, passwords, therefore another authentication measure is needed.

This is the reason multi-factor authentication is advised. It combines multiple measures together to have many layers of defence making it very difficult for an attacker. Back in 2017, a great overview by Dasgupta (et al.) in their book "Advances in User Authentication" highlights the main authentication measures that can be deployed (Dasgupta et al., 2017).

The most common types of authentication types are (Dasgupta et al., 2017):

- What the user knows – passwords.
- What the user has - authentication apps, SMS texts.
- What the user is – biometric information (E.G fingerprint).
- Where the user is – location information (E.G GPS).

To implement many layers of defence combining two of these authentication types will enable Two-Factor Authentication. For example, combining as a user's password (something the user knows) with an authentication app (what the user has) would be Two-Factor Authentication (2FA).

Authentication apps are a brilliant 2FA option as recommended by Dasgupta (et al.). They function by the user entering their password to authenticate the first layer. Then, a One-Time Password (OTP) is sent to their device in response to the login attempt (Dasgupta et al., 2017). The OTP is normally valid for around 30 to 60 seconds, and if the user is too slow to provide the code a new one will need to be generated.

Combining multiple types of authentication mechanisms will significantly improve the defensive layers of a company. A secure website should enforce 2FA where possible whilst also reducing the difficulty a user goes through to adopt the authentication measures.

Authentication recommendations

Recommendations

As identified in the literature review there are many authentication mechanisms that can be implemented to secure the web applications. The first recommendation that the IT manager recommends that ScottishGlen implement is create a log in system as it will be very familiar with staff already (Velásquez et al., 2018). Specifically, passwords should be required to log into the website as a first layer. Staff will create their account with a unique username and a password.

As discussed, staff should be taught how to create a secure password by choosing three random words (McCormack, 2016). Also, it's important that staff don't make it easily guessable either as you would with any password. No personal or relatable words that the hacktivists may try to guess. Brining back the previous example, "grassempiremoney is suitable as it has no relation to ScottishGlen or any staff member. The password requirements should only have a minimum password length of 8 characters (guideline) and if the budget can handle it to not limit password length. This will allow staff to create strong memorable passwords.

On the account creation page of the company website, it should have a simple web design to authenticate with clear messages on instructions to meet the password policy. It's also beneficial to replace the "Sign Up" and "Sign In" with "Sign Up" and "Log In" which helps interface design (Bozor.io, 2018). User's should be notified of what objectives they've met in the password policy such as the password length when trying to create their password. However, this is only one layer and if an attacker guesses/obtains the password the website will be compromised with the hacktivists able to launch further attacks from the staff account.

The second recommendation is that Two-Factor Authentication (2FA) is implemented as well. Considering the budget constraints, if possible, all staff should be supplied with a company phone if one is not provided to further make ScottishGlen resilient against the hacktivists attack and reduce overall attack surface. An authentication app should be installed on this phone by each staff member which will generate the One Time Passcode (OTP) for 2FA authentication when signing in. Google Authenticator is a free two-factor authentication application that can be installed onto the smartphone and available in the Google Play and Apple App store. You do not need a google account to use it. Staff will simply link the authentication app to their website account, and it will start automatically generating timed unique OTP codes (Rogers, 2023).

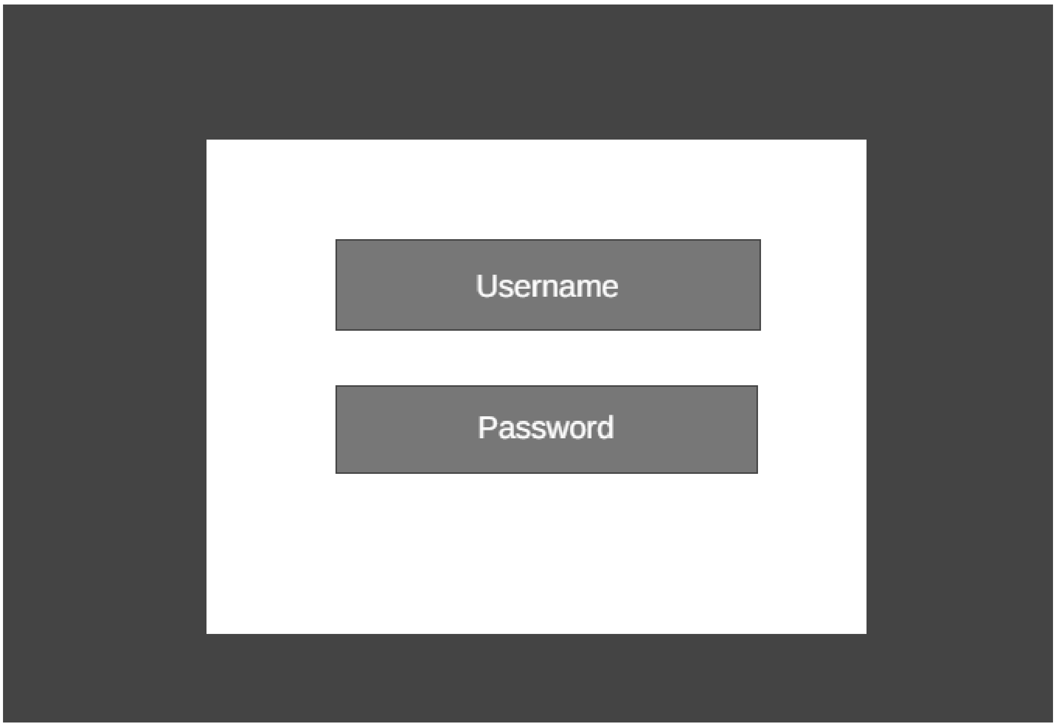
This is a cost-effective approach to the threat posed by the insecure internal web apps enabling multiple security layers for the website whilst still making it easy and usable for the staff (Catherine S. Weir, 2010). Biometrics would be too costly to implement with the limited budget. Password managers are far more difficult for staff to learn and adopt so was not recommended. Once these authentication measures are implemented the hacktivists' attempts to gain access to the internal web apps will be significantly disrupted and near impossible.

Wireframe Designs

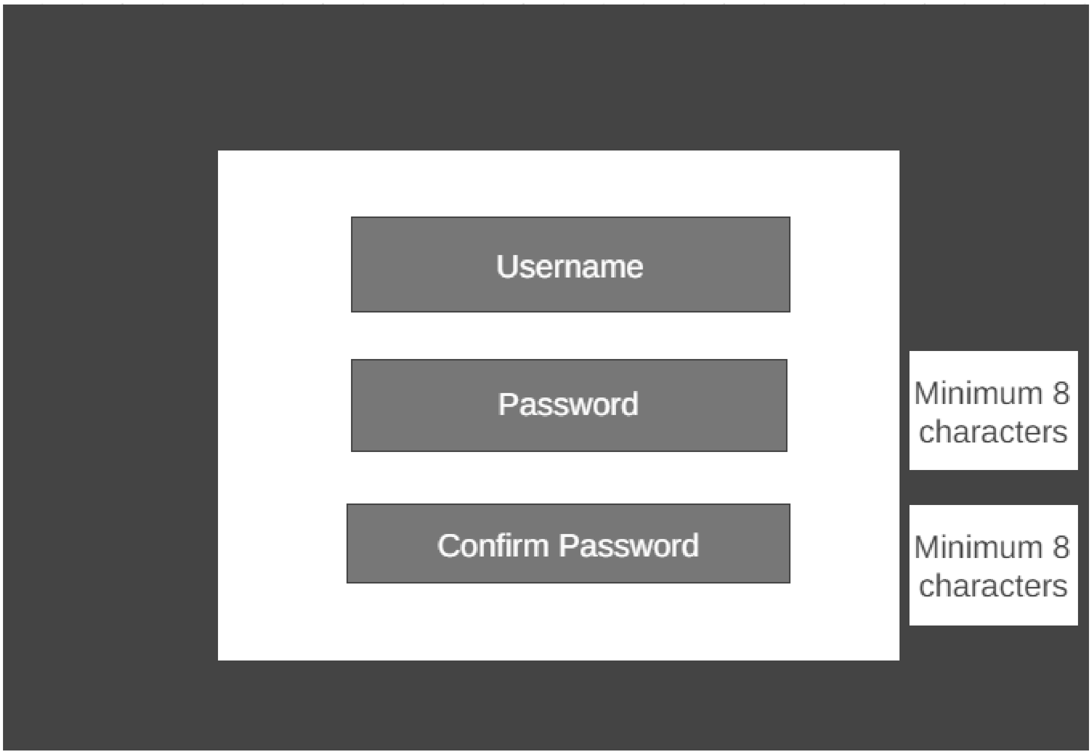
The IT manager would like to show an example of what the authentication recommendations may look like for better understanding on how to implement them accurately. Wireframe diagrams, found on the next pages, have been created on each part of the web application that a user will encounter when authenticating.

Log In system

User Log In

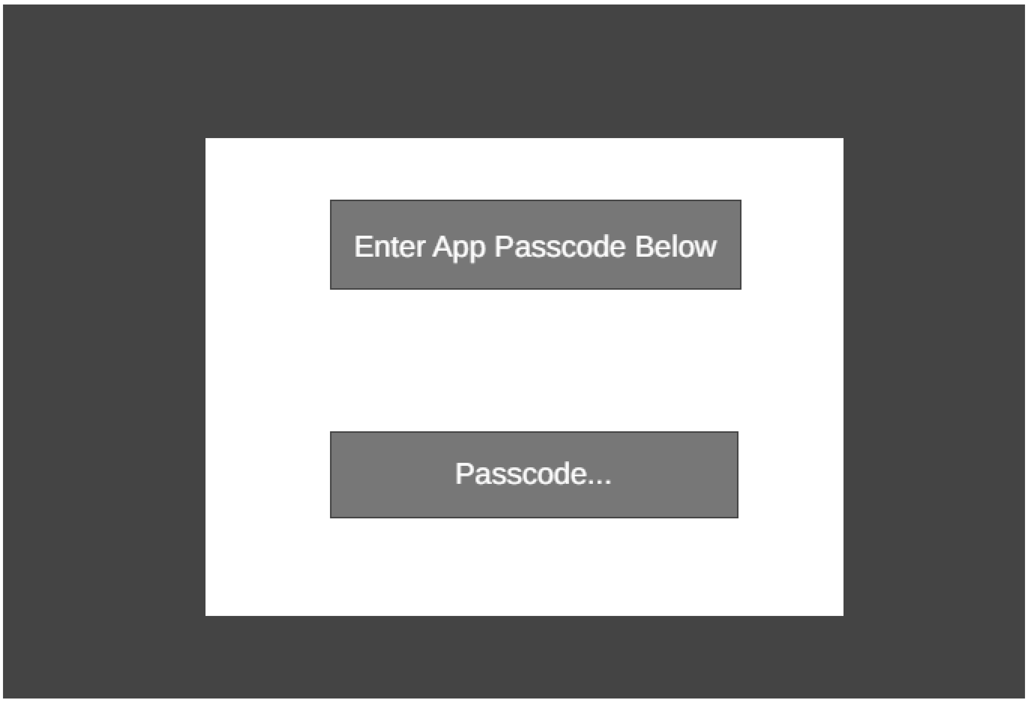


User Changing Password



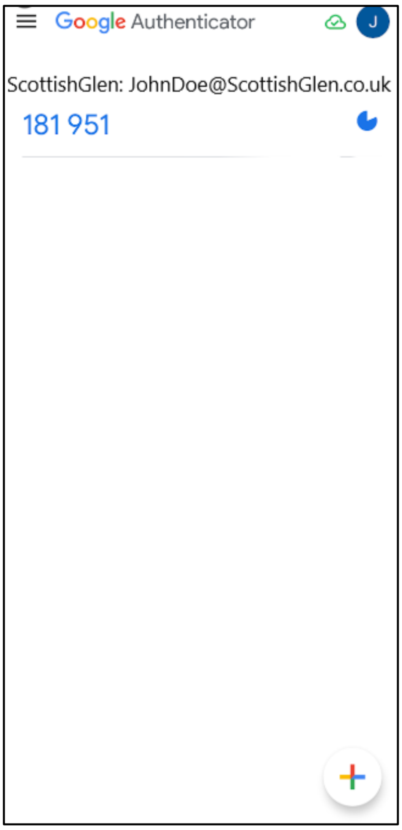
Enter OTP number interface

Web App requesting passcode to authenticate session



Authentication App generating code

Google Authenticator generating OTP for John Doe

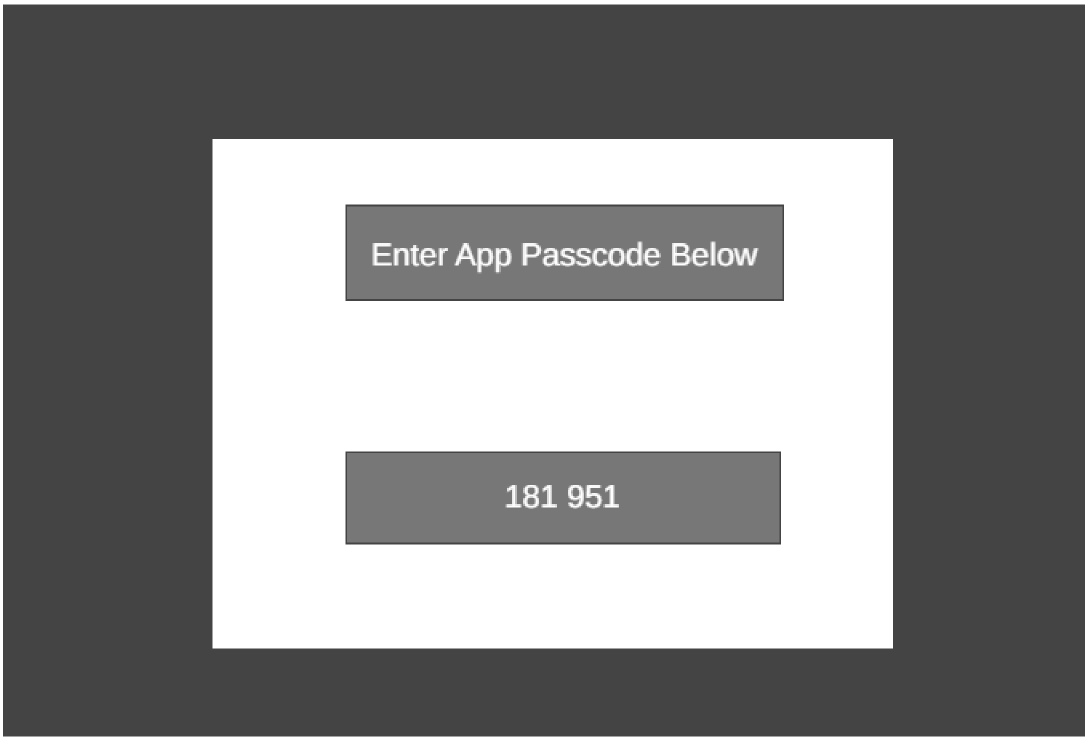


ScottishGlen: JohnDoe@ScottishGlen.co.uk

181 951

Entering in OTP on website

OPT entered in web app



References

Ankit Kumar Jain & B.B. Gupta, 2022, A survey of phishing attack techniques, defence mechanisms and open research challenges, Enterprise Information Systems, 16:4, 527-565, DOI: 10.1080/17517575.2021.1896786

Bozor.io, 2018, The Essential Guide to Enterprise Login and sign up UX and UI, Medium. Available at: https://medium.com/ux-station/the-essential-guide-to-enterprise-login-and-sign-up-ux-and-ui-a40c67d047a [Accessed: 23 May 2023].

Catherine S. Weir et al., 2010 Usable security: User preferences for authentication methods in eBanking and the effects of experience, Interacting with Computers, Volume 22, Issue 3, Pages 153–164, https://doi.org/10.1016/j.intcom.2009.10.001

Chrisda et al., 2023, Configure anti-phishing policies in Microsoft Defender for Office 365 - office 365, Office 365 | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-mdo-configure?view=o365-worldwide [Accessed: 21 May 2023].

Chrisda et al., 2023, Microsoft recommendations for EOP and defender for office 365 security settings - office 365, Microsoft recommendations for EOP and Defender for Office 365 security settings - Office 365 | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365#anti-phishing-policy-settings-in-microsoft-defender-for-office-365 [Accessed: 21 May 2023].

Dasgupta, D., Roy, A., Nag, A, 2017, Multi-Factor Authentication. In: Advances in User Authentication. Infosys Science Foundation Series(). Springer, Cham. https://doi-org.libproxy.abertay.ac.uk/10.1007/978-3-319-58808-7_5

Gordon, W.J. et al., 2019, ‘Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system’, Journal of the American Medical Informatics Association : JAMIA., 26(6), pp. 547–552. doi:10.1093/jamia/ocz005.

Gupta, B.B., Tewari, A., Jain, A.K. et al., 2017, Fighting against phishing attacks: state of the art and future challenges. Neural Comput & Applic 28, 3629–3654. https://doi-org.libproxy.abertay.ac.uk/10.1007/s00521-016-2275-y

Hong, J, 2012, ‘The state of phishing attacks’, *Communications of the ACM*, 55(1), pp. 74–81. doi:10.1145/2063176.2063197.

McCormack, I, 2016, Three random words or #thinkrandom, NCSC. Available at: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0 [Accessed: 23 May 2023].

NCSC, 2018, Password policy: Updating your approach, NCSC. Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach [Accessed: 23 May 2023].

NCSC, 2022, Phishing attacks: Defending your organisation, NCSC. Available at: https://www.ncsc.gov.uk/guidance/phishing [Accessed: 20 May 2023].

OWASP, 2021, A07:2021 – identification and authentication failures, A07 Identification and Authentication Failures - OWASP Top 10:2021. Available at: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ [Accessed: 23 May 2023].

Ramzan, Z, 2010. Phishing Attacks and Countermeasures. In: Stavroulakis, P., Stamp, M. (eds) Handbook of Information and Communication Security. Springer, Berlin, Heidelberg. https://doi-org.libproxy.abertay.ac.uk/10.1007/978-3-642-04117-4_23

Rogers, R, 2023, How to use Google Authenticator, Wired. Available at: https://www.wired.com/story/how-to-use-google-authenticator-app/ [Accessed: 23 May 2023].

Velásquez, I., Caro, A. and Rodríguez, A, 2018, 'Authentication schemes and methods: A systematic literature review', Information and software technology, 94, pp. 30–37. doi:10.1016/j.infsof.2017.09.012.