

Part 3. Human-Centred Security

Martin Georgiev

1901560

1. Human-Centred Risks

Phishing attacks pose a significant threat to human-centred security. Such attacks can be targeted (spearphishing) or through mass distribution (sending emails or SMS to numerous users or companies). The objective of phishing is to deceive users into opening a malicious link or file, leading to the download and execution of malware, directing them to a counterfeit website to extract their personal information, or a combination of both. Due to the challenges of automated detection, an organisation's employees serve as the crucial frontline defence against such attacks. Staff members are responsible for identifying and promptly reporting phishing attempts (NCSC, 2018).

Phishing attacks have significantly risen in recent years, primarily due to the COVID-19 pandemic lockdown and the shift towards home-office work. The pandemic fears and increased online activity have given adversaries more opportunities for social engineering attempts (Akdemir and Yenal, 2021). Phishing emails have become more diverse, encompassing monetary gain scams and false information concerning the virus. According to CheckPoint's report, 3% of the analysed domains were identified as malicious, aiming to install malware or steal user data, while 5% were considered suspicious. Additionally, there has been a notable surge in malicious email activity (CheckPoint, 2020). This rise is further supported by a survey conducted by the UK government, which revealed that 83% of the businesses surveyed had encountered phishing attacks (UK Government, 2021).

Phishing, being primarily associated with human factors, is considered a social-based security risk that relies heavily on appropriate human interaction for a successful defence. This statement is further emphasised through the phishing attack anatomy analysis (Alkhalil et al., 2021) and consumer psychology (Jakobsson, 2007). Urgency, authority, and fearmongering are three of the most common stimuli employed by phishing threat actors. Additionally, based on Jakobsson's survey, users gain more trust with personalised emails and judge their relevance before assessing their authenticity. While Jakobsson's survey also demonstrated that users could identify phishing scams based on grammar, spelling, and design, many modern phishing attempts are crafted to appear authentic. According to Desolda, resources, lack of awareness, and knowledge were the three primary factors exploited by cyber criminals (Desolda et al., 2022). As phishing is a social-based issue and threat actors employ emotional stimuli, users may react impulsively based on the contents of the email without recognising its authenticity (Hadlington, 2017).

To mitigate such issues, the organisation's executives should ensure that their employees are adequately trained and aware of modern phishing practices. Considering those factors, the organisation needs to consider the behaviour and emotions of its employees.

2. Human-Centred Recommendations

Security recommendations can be classified into three control categories: formal, informal, and technical. Regarding formal training, the investigator recommends establishing comprehensive security plans and policies while offering employee support. These plans and policies should encompass incident response, allocation of responsibilities, and risk management. They play a crucial role in preventing, identifying, and recovering from potential cybersecurity attacks.

One highly effective method of informal training is educating users about phishing practices through hands-on training, specifically focusing on phishing trends and email/website recognition. However, to ensure its effectiveness, the organisation needs to tailor the training to the demographics of its users, considering factors such as technical background and age. The company could either develop its phishing practice exercises or utilise third-party resources while closely

monitoring user actions such as clicked links, opened files and the number of reported emails, as well as the data they provide, including sensitive corporate information like user credentials or personal data. The training can also be designed in a gamified format, incorporating role-playing elements. This approach would allow users to learn from their mistakes while encouraging them to ask questions and seek clarification when uncertain (Wen et al., 2019). Additionally, users should receive proper education on phishing risks within a home-office environment.

Although the responsibility of identifying phishing attempts primarily rests with the users, the technical controls could assist employees through software solutions. Two notable applications in this regard are Microsoft Defender's anti-phishing protection (Microsoft, 2007) and Barracuda Sentinel (Barracuda, 2017). While Barracuda Sentinel offers a range of AI-powered features such as brand protection, domain fraud detection, and business email compromise prevention, the investigator suggests Microsoft's solution due to its greater flexibility. Additionally, Microsoft's software enables administrators to conduct phishing campaigns without specialised software or costly third-party services.

Considering that several employees have already received phishing emails from the alleged hacktivist group, it is highly recommended to promptly deploy anti-phishing software and training. The organisation should also reconsider the previously suggested software and training, scaling them appropriately as the organisation grows. Given the current size of Scottish Glen, Microsoft Defender would provide the organisation with adequate protection. However, as the organisation expands, alternative solutions like the recommended Barracuda Sentinel may become more suitable. Such measures would enhance the company's human-centred resilience. While the abovementioned methods would potentially mitigate phishing attempts, the researcher suggests evaluating the organisation's authentication mechanisms to enhance security and usability.

3. Authentication Mechanisms

According to Bonneau's research, authentication mechanisms can be evaluated based on usability, deployability, and security (Bonneau et al., 2012). However, the effectiveness of each criterion depends on the specific use case. Passwords remain the most prevalent authentication mechanism, and their usage continues to increase due to the rapid increase of devices and online services (NCSC, 2022). Bonneau's study compared various authentication methods to passwords and found that each authentication method offers different advantages in different scenarios, without any of them being definitively superior or inferior to passwords in terms of performance. Moreover, the suggested alternative methods did not demonstrate better or worse performance in terms of deployability. (Figure 3.1)

Category	Scheme	Described in section	Reference	Usability					Deployability				Security														
				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]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Password managers	Firefox	IV-A	[22]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	LastPass		[42]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Proxy	URRSA	IV-B	[5]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Impostor		[23]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Federated	OpenID	IV-C	[27]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Microsoft Passport		[43]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Facebook Connect		[44]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	BrowserID		[45]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Graphical	OTP over email	IV-D	[46]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	PCCP		[7]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Cognitive	PassGo	IV-E	[47]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	GrIDsure (original)		[30]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Weinshall		[48]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Hopper Blum		[49]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Paper tokens	Word Association	[50]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○
	OTPW	IV-F	[33]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	S/KEY		[32]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Visual crypto	PIN+TAN	[51]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○
	PassWindow	[52]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○
Hardware tokens	RSA SecurID	IV-G	[34]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Yubikey		[53]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Ironkey		[54]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	CAP reader		[55]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Phone-based	Pico	[8]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○
	Phoolproof	IV-H	[36]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Cronto		[56]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Biometric	MP-Auth	IV-I	[6]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○
OTP over SMS		[57]		●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Google 2-Step		[57]		●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Recovery	Fingerprint	IV-I	[38]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Iris		[39]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Voice		[40]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
Recovery	Personal knowledge		[58]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Preference-based		[59]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
	Social re-auth.		[60]	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○

● = offers the benefit; ○ = almost offers the benefit; no circle = does not offer the benefit.
|||| = better than passwords; ||||| = worse than passwords; no background pattern = no change.

● = offers the benefit; ○ = almost offers the benefit; no circle = does not offer the benefit.
 ■ = better than passwords; ■ = worse than passwords; no background pattern = no change.

Figure 3.1 – Categories and mechanisms in Bonneau’s study.

However, passwords cannot be entirely relied upon and have their limitations. They are user-created and serve as knowledge-based secrets. The necessity of managing multiple accounts usually leads users to reuse old passwords or predictable patterns, rendering them vulnerable to attacks like brute forcing. Moreover, passwords pose challenges for individuals with dyslexia and require multiple cognitive abilities (Renaud et al., 2021). Remembering numerous distinct passwords could also be difficult, often resulting in forgetting them and potentially locking the accounts. Password managers can be employed to address these issues. Nevertheless, **password managers** rely on a master password, and forgetting it would pose significant difficulties or even make it impossible to retrieve any stored credentials. Furthermore, password managers may not be suitable in corporate settings, as all sensitive data would be consolidated in one location, making it an easier target for attackers.

Despite the accessibility issues associated with passwords, they would be a more suitable choice for Scottish Glen's current scenario. Passwords would not pose any deployability concerns and most personnel could utilise them. Although other authentication methods identified in Bonneau's research might seem more secure, their usability and deployability are often inferior, potentially requiring considerable time for implementation and staff training in their workplace. As recommended by the NCSC, the organisation could combine passwords with additional

authentication mechanisms like Multi-Factor Authentication (from here on **MFA**), **OAuth 2.0**, **FIDO2**, or **magic links/one-time passwords**.

Among the proposed mechanisms, **MFA** would be the most common and the investigator's recommended method. While the other authentication methods may also be effective, they would be more suitable in different scenarios – **OAuth 2.0**, when users can sign in with personal accounts, **magic links** for accessibility over security, and **FIDO2** for enhanced security. However, **OAuth 2.0** could pose additional security risks if the hacktivist group manages to infiltrate a staff member's personal Google/Apple account, granting them access to the corporate network. Although magic links would enhance accessibility for dyslexic users, there is a risk of social engineering attempts to obtain the link or one-time password and gain unauthorised access. **FIDO2** offers the highest level of security by utilising a physical cryptographic key, typically a **USB device**. Users can insert it when prompted for automated authentication. However, implementing **FIDO2** could be costly if the company expands.

MFA could be achieved using applications such as Google Authenticator or Microsoft Authenticator. The investigator recommends the latter option as it is available with Microsoft 365 and can be installed on Android/iOS smartphones. Users can utilise it after an administrator links it to a company mobile phone or the staff member's device. During a login attempt, the user will receive a push notification. From there, they can choose how to authenticate depending on their configured options (Microsoft, 2023):

- Biometrics: Fingerprints, facial recognition, etc.
- Authentication number: Provided by the login form, users need to press it within the authentication app.
- One-time passcode: A randomly generated key within the mobile app. It remains valid for a short period and can be inserted into the login form for authentication.

The organisation could combine the tool with passwords to enhance security and provide multiple layers of defence. They could also employ it as a standalone authentication service without passwords. Users would then just require a username and one of the previously mentioned authentication methods, significantly improving accessibility for users with dyslexia. This, however, would require phishing/social engineering awareness training as threat actors are known to spam notifications and staff members could accidentally accept it.

Considering the previously mentioned drawbacks of OAuth 2.0, FIDO2, and magic links, the researcher would base their recommendations on a combination of passwords and MFA.

4. Authentication Recommendations

As Scottish Glen is currently being targeted by a hacktivist organisation and their internal applications do not require employee authentication, the authentication measures should focus on security. Combining passwords with MFA would interfere with possible breaches and brute-forcing techniques. The recommended mechanism will answer the three key authentication factors:

- *Something you **know*** – User-generated password.
- *Something you **have*** – Device with Microsoft Authenticator.
- *Something you **are*** – User biometric data.

Implementing the authentication mechanism would guarantee the company's network security is secure, even in the event of potential user credential theft. Beginning with the "*something you*

know" aspect, staff members will be prompted to create a password adhering to specified guidelines. To ensure password strength, the investigator advises employing an interactive guide that dynamically evaluates the user's input. The live checklist would display the password's strength in real-time, accompanied by a locked/unlocked lock symbol indicating when the password meets the required level of robustness. The researcher proposes the following set of rules (Microsoft, 2023):

- Password must be at least 10 symbols long.
- Password must include alphanumeric and special characters (!@#\$%^&*).
- Password must include at least one small and capital letter.
- Must not use common passwords/words – i.e., "password123!".
- It is recommended to use easy-to-remember but difficult-to-guess passphrases – i.e., "Av3ryStRONGP@sswoRD!".

Regarding the "something you have" and "something you are" aspects, staff members need to authorise the login requests from their mobile devices equipped with Microsoft Authenticator. This device covers the former requirement, while the latter would be applicable if the user has set up fingerprint (or other biometric) authentication. The registration, login, and password-change process would consist of the following stages:

- The administrator generates a temporary password.
- The administrator configures Microsoft Authenticator on the organisation's designated mobile device assigned to the staff member.
- The staff member receives the password, a link to change the password, and the device.
- The user proceeds to change the password, guided by live strength indicators.
- The user confirms the process through the Authenticator app.
- Optionally, the user can modify the configured MFA setting to utilise biometric data (i.e., fingerprint).


Regarding the sign-in page, users will be prompted to enter their username and password. Upon clicking the sign-in button, the first authentication step of password verification is initiated. Entering the valid password would trigger a push notification on the user's device. The user is then required to approve the login request from their device, reducing the effectiveness of password guessing and phishing attempts. Staff members should still receive comprehensive training on identifying and mitigating phishing and social engineering attacks to ensure the effectiveness of both security layers. Furthermore, the login page should include a "forgotten password" button, which directs users to the password reset page to change their temporary password.

The wireframe images (MockFlow, 2008) below can be used as guidance for the development of the mechanism (**Figures 4.1, 4.2, and 4.3**):


Password Reset

Username:

Current Password:

New Password: 

- ✓ Password must be at least 10 symbols.
- ✓ Password must include alphanumeric and special characters (i.e., !@#\$%^&*_)
- ✓ Password should not contain common passwords/words.
- ✗ Password must include at least one small and capital letter.
- ✗ Password must not be the same as your previous one.

Repeat Password: 

✗ Passwords do not match.

Easy-to-remember but difficult-to-guess passphrases are recommended - (i.e., "Av3ryStR0NGP@sswoRD!").

Change Password

Figure 4.1 – Password change screen.



ScottishGlen

Username:

Password:

Login

Forgotten Password

Figure 4.2 – Login screen.

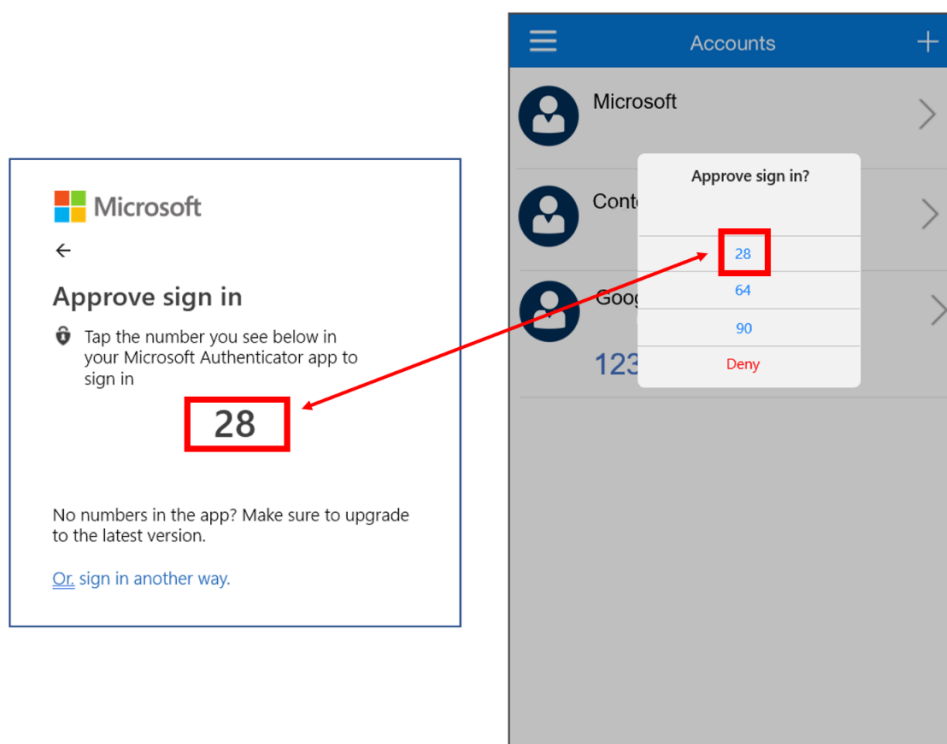


Figure 4.3 – Authentication number example (Ferreira, 2021).

Though this approach is not recommended until the staff is properly trained, the organisation could also utilise Microsoft Authenticator as a **passwordless** option, significantly enhancing accessibility for users with disabilities. Given the absence of authentication measures for internal applications at Scottish Glen, the investigator strongly advises immediate implementation of the recommended MFA authentication mechanism. Assigning a unique username to each staff member and combining it with a **strong password** and **Microsoft Authenticator** would mitigate brute-force techniques, substantially impeding phishing and social engineering attempts.

References

- NCSC (2018). *Phishing attacks: defending your organisation*. Available at: <https://www.ncsc.gov.uk/guidance/phishing/> (Accessed: 17 May 2023).
- Akdemir, N. and Yenal, S. (2021). *How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails*. *SAGE Open*, 11(3), p.215824402110318. doi:<https://doi.org/10.1177/21582440211031879/> (Accessed: 17 May 2023).
- CheckPoint (2020). *Update: Coronavirus-themed domains 50% more likely to be malicious than other domains*. Available at: <https://blog.checkpoint.com/security/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/> (Accessed: 17 May 2023).
- UK Government (2021). *Cyber Security Breaches Survey 2021*. Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021> (Accessed: 18 May 2023).
- Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3(1). doi:<https://doi.org/10.3389/fcomp.2021.563060/> (Accessed: 18 May 2023).
- Jakobsson, M. (2007). *The Human Factor in Phishing*. Available at: <http://markus-jakobsson.com/papers/jakobsson-psci07.pdf> (Accessed: 18 May 2023).
- Desolda, G., Ferro, L.S., Marrella, A., Catarci, T. and Costabile, M.F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, 54(8), pp.1–35. doi:<https://doi.org/10.1145/3469886/> (Accessed: 19 May 2023).
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), p.e00346. doi:<https://doi.org/10.1016/j.heliyon.2017.e00346/> (Accessed: 20 May 2023).
- Wen, Z.A., Lin, Z., Chen, R. and Andersen, E. (2019). What.Hack. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. doi:<https://doi.org/10.1145/3290605.3300338/> (Accessed: 20 May 2023).
- Barracuda (2017). *Baraccuda Sentinel*. Available at: <https://www.barracuda.com/products/email-protection/phishing-protection/> (Accessed: 20 May 2023).
- Microsoft (2007). *Microsoft Defender*. Available at: <https://www.microsoft.com/en-gb/security/business/microsoft-defender/> (Accessed: 20 May 2023).
- Bonneau, J., Herley, C., Oorschot, P.C. van and Stajano, F. (2012). *The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*. *IEEE Xplore*. doi:<https://doi.org/10.1109/SP.2012.44/> (Accessed: 20 May 2023).
- NCSC (2022). *Authentication methods: choosing the right type*. Available at: <https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type/> (Accessed: 20 May 2023).
- Renaud, K., Johnson, G. and Ophoff, J. (2021). Accessible authentication: dyslexia and password strategies. *Information & Computer Security*, 29(4), pp.604–624. doi:<https://doi.org/10.1108/ics-11-2020-0192> (Accessed: 21 May 2023).

Microsoft (2023). *Passwordless authentication options for Azure Active Directory*. Available at: <https://learn.microsoft.com/en-gb/azure/active-directory/authentication/concept-authentication-passwordless#microsoft-authenticator/> (Accessed: 21 May 2023).

Microsoft (2023). *Create and use strong passwords*. Available at: <https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb/> (Accessed: 21 May 2023).

MockFlow (2008). *MockFlow*. Available at: <https://www.mockflow.com/> (Accessed: 21 May 2023).

Ferrerira, J. (2021). *Microsoft Authenticator code matching for MFA notifications*. Available at: <https://m365admin.handsontek.net/microsoft-authenticator-code-matching-for-mfa-notifications/> (Accessed: 21 May 2023).