

LCLM4002 Digital Skills

Task 2 – Informative Poster

Student Name: Maria Mihaylova

Student ID: 2322624



Introduction

Digital technology allows connections without proximity. Due to the growing number of internet threats and risks, basic digital safety must be prioritised. This poster emphasises digital footprint protection basics. Understanding and applying digital security principles will protect individuals and organisations online. The poster covered password security, phishing awareness, software updates, social media privacy, and 2FA implementation.

Discussion on Digital Safety Measures

Password Security

The most important way to secure online communication is with passwords. Unique character combinations are needed for secure passwords. Uppercase and lowercase letters, numerals, and symbols should be included. One should avoid sharing predictable information like favourite name or birthday. Using popular password managers can also boost security. These software applications protect passwords and simplify account management (Allahrakha, 2023). Unauthorised access to personal online accounts is greatly reduced.

Software Updates

Regularly installing software updates enhances the robustness of digital information security measures. To rectify software glitches and thwart emerging security risks, it is imperative to regularly update operating systems and antivirus software. Configure devices to automatically receive updates whenever feasible. Enabling automatic updates is a method to ensure the security of digital tools. Users can safeguard their digital assets by adhering to trustworthy security updates (Keshta, and Odeh, 2021). Prioritising software updates can enhance cyber security.

Social Media Privacy

Social media facilitates interpersonal connections and enables the exchange of information. Nevertheless, the incorrect utilisation of these services can jeopardise privacy. Review and modify privacy settings to restrict the visibility of personal information and posts. Online information is accessible to a wide audience, including potential employers and advertisers. Individuals must exercise caution regarding their online audience when sharing information. People should exercise caution when accepting friend requests or sharing personal information with strangers to safeguard privacy and identity (Atlam and Wills, 2020).

Two-Factor Authentication (2FA)

Implementing two-factor authentication (2FA) greatly enhances the security of online accounts. Verification necessitates more than just a password. There are numerous strategies to enhance identification processes. These options encompass SMS codes, authenticator software, and biometric verification. Implementing two-factor authentication can effectively mitigate the risk of unauthorised access in the event of a forgotten or stolen password (Gupta et al., 2020). Implementing two-factor authentication (2FA) enhances the security of all online accounts.

Phishing Awareness

Phishers send fake emails, SMS messages, and phone calls to random recipients. These texts trick people into phishing. Staying current on hacking strategies helps avoid these scams. Someone soliciting personal information without consent requires caution. Before sharing sensitive

information, people should verify its source (Jain et al., 2021). Protecting sensitive data is essential. Spelling errors, unusual sender addresses, and prompt responses warrant further investigation. Phishing attempts can be reduced by being wary of unknown messages.

Conclusion

This poster emphasises digital safety basics and trends. Use strong passwords, monitor for fraud, update software, manage social media privacy settings, and use two-factor authentication. Today, digital transactions are part of our daily lives, so learning and using technology securely is crucial. We must protect our identities and confidential information to succeed in the digital age. Protecting digital data is paramount.

References

- Allahrakha, N., 2023. Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Legal Issues in the Digital Age*, 4(2), pp.78-121.
- Atlam, H.F. and Wills, G.B., 2020. IoT security, privacy, safety and ethics. *Digital twin technologies and smart cities*, pp.123-149.
- Bruzgiene, R. and Jurgilas, K., 2021. Securing remote access to information systems of critical infrastructure using two-factor authentication. *Electronics*, 10(15), p.1819.
- Gupta, M., Abdelsalam, M., Khorsandroo, S. and Mittal, S., 2020. Security and privacy in smart farming: Challenges and opportunities. *IEEE access*, 8, pp.34564-34584.
- Jain, A.K., Sahoo, S.R. and Kaubiyal, J., 2021. Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), pp.2157-2177.
- Keshta, I. and Odeh, A., 2021. Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), pp.177-183.