



Basic Digital Safety

Name: Valentin Hulub
Student ID: 2316682



Introduction

As digital technologies become increasingly ingrained in our professional lives, the importance of digital safety within the workplace cannot be overstated. Protecting organisational assets from cyber threats is not just about technology—it's about fostering a culture of awareness and resilience. A robust digital safety protocol is essential to defend against the ever-growing spectrum of cyber threats, from phishing to data theft, ensuring the security of both employee and company data (Hadlington, 2017; Jang-Jaccard & Nepal, 2014).

Secure Passwords and Authentication



Strong passwords act as the first line of defence in digital safety. They should be complex, combining letters, numbers, and symbols, and changed regularly to prevent unauthorised access. Multi-factor authentication adds security layer, requiring two or more verification methods, significantly reducing breach risks (Stewart, 2018). This dual approach to password security is a cornerstone in safeguarding personal and organisational data against cyber intrusions.

Regular Updates and Anti-Virus Protection

Keeping software and systems updated is vital in digital safety. Updates often include patches for security vulnerabilities that cybercriminals could exploit. Alongside regular updates, robust anti-virus software can detect and mitigate threats, offering real-time protection against malware and other cyber threats (Hadlington, 2017). Regularly scheduled scans and updates form a proactive defense strategy, essential for maintaining digital safety in the workplace.

Employee Education and Data Encryption



A collection of unprocessed numbers or characters is known as raw employee education, which is crucial in recognising and preventing cyber threats. Regular training sessions on digital safety can empower employees to identify and appropriately respond to threats such as phishing (Wombat Security, 2019). Additionally, data encryption should be employed to protect sensitive information, ensuring that even if data is intercepted, it remains unreadable and secure from unauthorised access (Sookhak et al., 2017).

Conclusion

Adopting rigorous digital safety practices is essential to safeguarding the workplace in the digital age. By prioritizing strong passwords, regular updates, and continuous employee education, businesses can create a secure digital environment resilient to evolving cyber threats.

References

1. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.
2. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.
3. Sookhak, M., Gani, A., Khan, M. K., & Buyya, R. (2017). Dynamic remote data auditing for securing big data storage in cloud computing. *Information Sciences*, 380, 101-116.
4. Wombat Security. (2019). State of the Phish Report. Wombat Security Technologies.
5. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.
6. Stewart, J. (2018). *Cybersecurity: An essential guide to computer and cyber security for beginners, including ethical hacking, risk assessment, social engineering, attack defense strategies, and much more*. Independently Published.