

Basic Digital Safety

What is Basic Digital Safety?

Basic Digital Safety aims at the safety precautions that are taken and practices applied to ensure a better defense against cyber threats like phishing, hacking, identity theft, and malware (Perwej *et al.*, 2021). Its essence is awareness of how data is transferred, stored and used across digital environments and media.

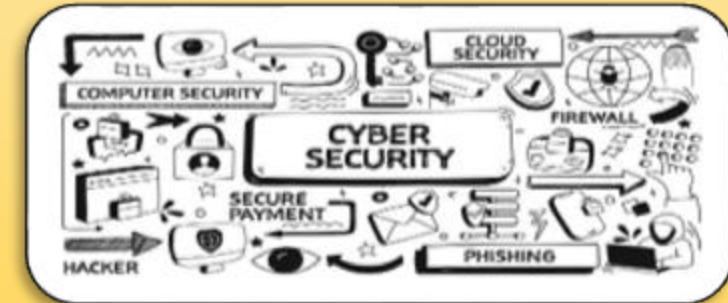


Importance of Basic Digital Safety

In this digital world, where nearly everything is done digitally, digital safety is inevitable. It protects sensitive information such as personal identification details, financial data, as well as passwords from attackers. Digital safety has also been successful in preventing identity theft, protecting against cyberbullying, and minimizing exposure to harmful or inappropriate content (Barbhuiya, 2024). For businesses, maintaining digital safety will ensure that they comply with data protection laws and regulations and basically gain customers' trust because of a commitment to their privacy and security. For an individual, it greatly enhances privacy and peace of mind, considering that online interactions and information are secure.

Types of Basic Digital Safety

- **Password Management:** Using strong and unique passwords for all accounts as well as activating two-factor authentication (2FA) to further secure the accounts (Jarecki *et al.*, 2021).
- **Safe Browsing Practices:** Avoid opening unfamiliar links, downloading files from unknown sources, and accessing insecure websites.
- **Anti-malware Software:** Installing as well as updating security software to protect devices from malicious programs (Samociuk, 2023).
- **Data Privacy:** Keeping personal data posted online to a minimum, and using privacy settings in social networking sites to limit access to personal data.
- **Phishing Awareness:** Be cautious of phishing emails or messages that intend to obtain personal data.
- **Secure Networks:** Using virtual private networks (VPNs) for any public Wi-Fi to encrypt data.
- **Regular Software Updates:** Ensuring every device and application is updated regularly to remove security vulnerabilities.



References

- Barbhuiya, R.K. (2024). Cyber-Safety: Concepts, Threats, and Essential Measures. *Indian Journal of Educational Technology*, 6(1), pp.361-376.
- Jarecki, S., Jubur, M., Krawczyk, H., Saxena, N. and Shirvanian, M. (2021). Two-factor password-authenticated key exchange with end-to-end security. *ACM Transactions on Privacy and Security (TOPS)*, 24(3), pp.1-37.
- Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N. and Jaiswal, A.K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, 9(12), pp.669-710.
- Samociuk, D. (2023). Antivirus evasion methods in modern operating systems. *Applied Sciences*, 13(8), p.5083.