

Protecting Your Digital Identity

With the current world being an internet-centric world, it is crucial to ensure that your online identity is secure. Among them, one of the initial measures is to use effective and distinctive passwords. Weichbroth and Łysik (2020) recommended, for instance, that a password should be at least 12 characters long, containing both lowercase and uppercase letters, numbers, and special characters. It is recommended to not use easily guessable personal data like your name and date of birth are used in the content. To be able to deal with the numerous accounts efficiently and securely, the use of a password manager can be highly efficient since it helps in generating and storing complex passwords.

Two-Factor Authentication (2FA)

To enhance your protection even more, it's vital to set up a two-factor authentication or at least use one-factor authentication. This kind of security measure call for another type of verification aside from a password, for instance, a code will be sent to your phone or fingerprint. According to Sule, Zennaro, and Thomas (2021), the adoption of 2FA ensures that the account is well protected even though the password may have been captured by the fraudster.

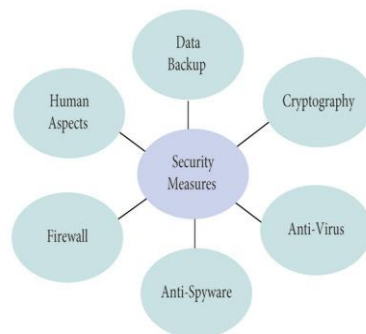
Phishing Awareness and Prevention

It is crucial to understand various phishing schemes as part of Internet security. Common message patterns in the use of phishing are messages that cause anxiety and express a sense of urgency and ask you to release personal details. Sule, Zennaro, and Thomas (2021) state that it is essential to be cautious and check whether the received e-mail or message is indeed from a legitimate sender when asking for personal identification information. Also, do not open links within emails, or any attachments you were not anticipating, or from addresses which look different than individuals or organizations you know but are a little off.



Device Security Measures

It is also important to ensure that your gadgets are safe from malicious attacks whether as a business, organization or as an individual. Smartphones, tablets, and computers should be protected by passwords or by fingerprints, face recognition, etc. Weichbroth and Łysik (2020) state that putting on new operating systems updating your devices and using reliable antivirus software helps in preventing cyber threats.



Managing Your Digital Footprint

Another procedural security control involves the control of one's digital footprint – the digital traces that one leaves behind. One should be considerably careful with the information he/she discloses personally, as this information can be used by criminals. According to Wu (2023), social networking user's privacy can be best safeguarded by setting proper boundaries as to whom their information is visible to hence, curtailing their exposure to the dangers.

Secure Browsing Habits

You have to ensure that you are practicing safe browsing in order to protect yourself from cyber threats. Wu (2023) also notes that you should ensure that the website you are communicating with is secure before proceeding to send information across; to do this, look for the padlock besides the HTTPS in the address bar as a sign that your information will be encrypted. Furthermore, one should be very careful and avoid, for example, clicking the links and pop-ups that appear to be malicious since these are often used by the attackers to obtain victims' data.

Staying Ahead of the Game in Malware Prevention



Your Digital Footprint

The digital world we live in is permanent and, with each post, you are creating a digital footprint. A **digital footprint** is the information that exists online about you and your activity.

HOW TO PRESERVE YOUR DIGITAL FOOTPRINT:

- Always think long term before posting
- Keep personal information private
- Use privacy settings on social networking pages
- Protect your privacy AND the privacy of your friends
- Apply the Golden Rule when online



Emergency Response Plan

It is also very important to always have a good and properly developed response plan in case of a security issue or threat. If your accounts get hacked, you need to understand how to act so that the losses would be reduced to a minimum. Some of the activities that one can engage in to improve their security are frequent data backup and always keenly observing their accounts for possible fraud activities (Sule, Zennaro, and Thomas, 2021).

Reference

Sule, M.-J., Zennaro, M. and Thomas, G. (2021). Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. *Technology in Society*, [online] 67(1), p.101734.

doi:<https://doi.org/10.1016/j.techsoc.2021.101734>.

Weichbroth, P. and Łysik, Ł. (2020). Mobile Security: Threats and Best Practices. *Mobile Information Systems*, 2020, pp.1–15. doi:<https://doi.org/10.1155/2020/8828078>.

Wu, H. (2023). Digital identity, privacy security, and their legal safeguards in the Metaverse. [online] *Ssrn.com*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4856096 [Accessed