

BASIC DIGITAL SAFETY

Name: Sandu Staris
I.D: 2323213
Group-2
Module name: Digital Skills
Module: LCLM4002

Basic digital safety is the concept of resilience against different risks related to the cybersecurity area of business operations. Identifying sources and activities for basic digital safety is important in a workplace because of the significant benefits that can be achieved, according to Yaacoub et al. (2020). Virus protection awareness and detection capability for malware installation can be identified as basic digital safety practices (Yaacoub et al., 2020). Basic digital safety practices are highly important because awareness about the current range of cyber security maintenance skills becomes possible once basic digital safety factors are considered (Yaacoub et al. 2020). The basic digital safety factor moves hand-in-hand with the adjacent element of information literacy. Basic digital safety factors and information literacy areas increase organisational capacity through the corresponding realisation of digital transformation and training requirements.



CHANGE YOUR PASSWORDS!

The first step that can be considered is continuously changing passwords at regular intervals (Zahra, 2023). Passwords can be complex based on the intensity of the safety requirement.



CERTIFICATIONS

Security certificates can also be adopted through proper verification and examination of the softwares used. Organisations can temporarily hire professionals to fulfil this action (Zahra, 2023).



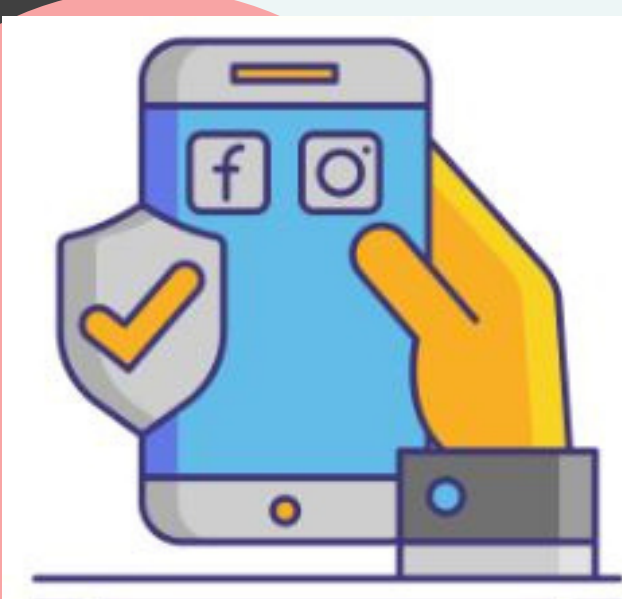
ONLINE PURCHASES

Another step that can be considered is maintaining safety while online purchases. Protecting sensitive information such as credit card or debit card data is necessary by not saving it. The systems can always present pop-ups digitally about saving the password and the Card Verification Value codes. Ignoring such unnecessary actions can lead to basic digital safety.



AI TOOLS

Another factor that can be considered is refraining from sharing information related to personal biodata and account numbers inside the Artificial Intelligence tools. Malware can remain installed inside the presented Artificial Intelligence tools, leading to the vulnerability of customer information. Such activities can be carried out inside the organisational premises.



SOCIAL MEDIA

Social media posts made by stakeholders in the work environment can become subject to malicious communicative messages which can contain certain hyperlinks. These hyperlinks can directly reset the systems and introduce certain trojan horses and viruses. Hence, carefulness has to be maintained while making limited social media posts (Pitardi and Marriott, 2021).

Conclusion

It can be concluded from the sections given above that there are different ways through which simple and efficient digital security can be improved in the workplace. The importance of the data associated with both customers and the other internal stakeholders, such as the company employees, must be realised accordingly. The password change processes, security certificate areas, AI tool usage facilities and malware installation through hyperlinks can be taken into account on this basis.

References

- Pitardi, V. and Marriott, H.R., 2021. Alexa, she's not human but... Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology & Marketing*, 38(4), pp.626-642. Available at: <https://doi.org/10.1002/mar.21457> [Accessed 2 April 2024]
- Pulido, C.M., Villarejo-Carballido, B., Redondo-Sama, G. and Gómez, A., 2020. COVID-19 infodemic: More retweets for science-based information on coronavirus than for false information. *International sociology*, 35(4), pp.377-392. Available at: <https://doi.org/10.1177/0268580920914755> [Accessed 2 April 2024]
- Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M., 2020. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, 77, p.103201. Available at: <https://doi.org/10.1016/j.micpro.2020.103201> [Accessed 2 April 2024]
- Zahra, N., 2023. Enhancing Inclusion in the National Digital Literacy Index: From Measurement to Empowerment. Available at: <https://repository.cips-indonesia.org/media/publications/567714-enhancing-inclusion-in-the-national-digi-843210f3.pdf> [Accessed 2 April 2024]