

Name: Junior Goncalves Pimenta

Student Number: 2415951

Module Code: LCLM4002

Module Title: Digital Skills

Lecturer Name: Rejwan Bin Sulaiman

Assignment Title: Digital Skills - Portfolio of tasks

Task 2

Basic Digital Skills



Introduction

In today's digital world, defending your online presence can be nothing short of vital. Cyber threats come forth in myriad forms every day, and being informed helps a person avoid becoming a victim. For this reason, here is a guide to understanding the most important threats and best practices that will keep you safe in the digital world



Stay Alert, Stay Secure!

What to Do If You Suspect a Breach

- ✓ Disconnect the internet right away to avoid further damage.
- ✓ Change the affected passwords, and, where available, enable 2FA.
- ✓ Report the issue to either IT support or the appropriate department immediately

Best Practices for Safety

1. **Use Strong Passwords:** Strong Passwords Use a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using easy passwords containing your name or a common phrase.
2. **Enable Two-Factor Authentication (2FA):** This is an additional security check that requires a verification from a second source of identification apart from your primary identification when logging in, for example, sending a code to your phone (Szczygieł, Florczak and Jasiak, 2023)
3. **Be Cautious of Suspicious Links:** Be cautious of suspicious links. Before clicking on the link, hover your mouse over the link and see where it leads you. Never click on any link or download attachments from an unknown sender.
4. **Update Software Regularly:** Most of the updates included security patches that would have upgraded your device to prevent a particular exploitation. Allow updates occasionally to update automatically.
5. **Secure Your Internet Connection:** Once surfing the net using free public Wi-Fi, use a virtual private network, or VPN to ensure encrypted browsing. Also, ensure that the password of your home Wi-Fi is strong and secure.



Key Threats

- **Phishing Scams-** These are fraudulent e-mails or messages with the intention of making a person disclose his sensitive information such as passwords or credit card numbers (Alkhalil et al., 2021).
- **Malware:** This refers to malicious software that can attack your device, steal your data, and breach your security.
- **Weak Passwords:** If you have simple passwords like "password123" or "qwerty," it's very easy for attackers to guess your passwords, and that puts your accounts at risk.



Refences

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, [online] 3(1), pp.1–23. doi:<https://doi.org/10.3389/fcomp.2021.563060>.
Szczygieł, I., Florczak, S. and Jasiak, A. (2023). Two-factor authentication (2FA) comparison of methods and applications. *Advances in Web Development Journal*, [online] 1(1). doi:<https://doi.org/10.5281/zenodo.10050024>.