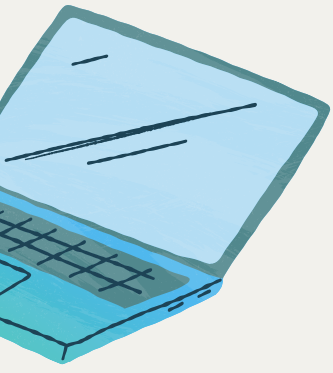


Digital Safety in the workplace

Alexandra Ivan
Student ID: 2330887



WHAT IS DIGITAL SAFETY?

- Protect personal and sensitive information.
- Safeguard against unauthorized access.
- Secure communication and data transfer.
- Awareness of online risks.
- Use passwords and encryption.



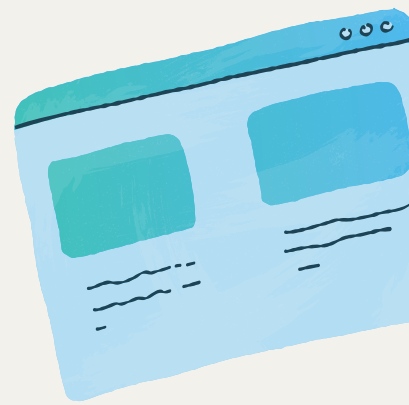
TYPES OF ONLINE THREATS

- Phishing: Fraudulent emails for information.
- Malware: Malicious software damaging systems.
- Ransomware: Malware locks data for ransom.
- Social Engineering: Manipulate for confidential information.
- DDoS Attacks: Overload for service disruption.



PROTECTION ONLINE CHILD SAFETY

- Educate children on internet safety.
- Use parental controls and monitoring.
- Open communication about online activities.
- Avoid sharing personal information.
- Secure social media settings.



ONLINE HACKING

- Unauthorized system or data access.
- Data breaches and identity theft.
- Methods: brute force, keylogging, exploiting.
- Targets weak passwords, outdated software.
- Proactive detection and prevention.

CONCLUSION



- Awareness and security reduce risks.
- Continuous education and vigilance needed.
- Everyone ensures a secure environment.

PREVENTION

- Strong & unique passwords.
- Authentication 2FA
- Regular software updates.
- Avoid suspicious links and attachments.

References:

- Jan A. (2014) Digital Skills. Unlocking the information society. Available at: <https://ebookcentral.proquest.com/lib/trinity/reader.action?docID=4828194>
- Kathy A. (2023) Literacy for digital futures. Available at: <https://library.oapen.org/handle/20.500.12657/75928>