

Andrew Omoregie | I.D2317934 |

04.04.2024

Digital Skills, LCLM4002 ,

Lecturer's Name: Amitave Banik

Basic Digital Safety

Have secure connections at all times

Public Wi-Fi is sometimes necessary but lacks good security control, making it vulnerable to cyberattacks. Avoid sensitive transactions like online banking or shopping. Use a Virtual Private Network (VPN) for real-time encryption. Save personal transactions until a trusted internet connection is available, as VPNs protect data over unsecured networks. (Kaspersky, 2020.)



Create a complex password

A strong password, combining numbers, uppercase and lowercase letters, and special characters, “example: oPbTdX5@4Rl87@td” is a crucial defence against hackers and malicious actors. It protects sensitive financial and personal information and prevents security breaches (Linkedin, n.d.) Change of password periodically helps protect your contain online.



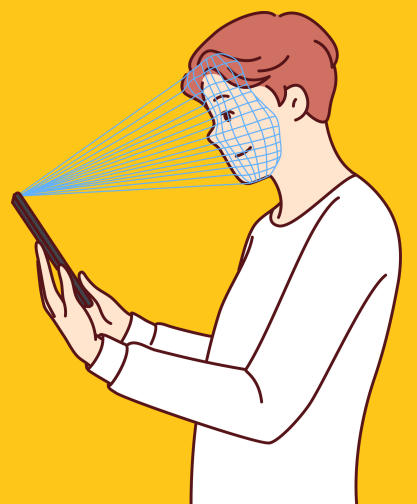
Keep Computer Updated

Developers continuously update products, monitor threats, and release security patches. Using the latest operating systems and apps is vital for sensitive user information. (Kaspersky, 2020)



Use Multifactor authentication whenever possible

More than one way verification protect sensitive information example multifactor authentication (MFA) is an authentication method that requires users to provide multiple verification methods, such as a one-time password, personal security questions, or biometric information. This will reduce the risk of being hacked by hackers. Example: when dealing with a bank, two ways verification is important to keep safe (Kaspersky, 2020).



Check website reability and avoid Suspicious Online Links

To assess a website's credibility, check its domain name, sources, contact page, design, and security connection. Look for citations, author's names, credentials, and sources. A well-designed website with professional design is more legitimate. Check for security indicators like HTTPS. You can also check on the

<https://www.getsafeonline.org/checkawebsite/> (Edge, 2023)
Reference



Kaspersky (2020). Top 10 Internet Safety Rules & What Not to Do Online. [online] Kaspersky.com. Available at: <https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online> (accessed 27.03.2024)

www.linkedin.com. (n.d.). The importance of a strong password: Safeguarding your digital world. [online] Available at: [https://www.linkedin.com/pulse/importance-strong-password-safeavailable at: https://www.microsoft.com/en-us/edge/learning-center/how-to-tell-if-a-site-is-credible?form=MA13I2](https://www.linkedin.com/pulse/importance-strong-password-safeavailable-at-https://www.microsoft.com/en-us/edge/learning-center/how-to-tell-if-a-site-is-credible?form=MA13I2). (accessed 27.03.2024)

Edge. (2023). How to Tell If a Website Is Credible | Edge Learning Center. [online] Available at: <https://www.microsoft.com/en-us/edge/learning-center/how-to-tell-if-a-site-is-credible?form=MA13I2> (accessed 27.03.2024)