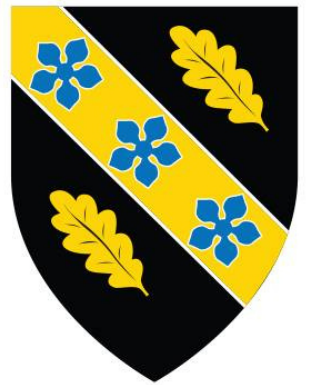


BASIC DIGITAL SAFETY



YOUR ONLINE IDENTITY AND PERSONAL DATA CAN BE PROTECTED BY FOLLOWING TO THESE BASIC DIGITAL SAFETY GUIDELINES.



1. STRONG PASSWORDS:

To prevent unwanted access, use strong and different passwords for every online account. Add a variety of special characters, numbers, and letters (Fedor, 2022).

2. PHISHING AWARENESS:

Be careful when clicking on dodgy emails, messages, or links as they might be attempts to obtain personal information through phishing scams. Avoid from clicking on unidentified links (Smith, 2021).



3. SECURE WI-FI:

To prevent hackers from accessing your data, make sure your home Wi-Fi network is encrypted and has a strong password (Smith, 2021).



4. SAFE BROWSING:

When entering sensitive information, such as passwords or credit card numbers, use secure websites (look for "https://" in the URL). (Chatzidrosos, 2024).



5. SOCIAL MEDIA CAUTION:

Be careful when sharing things on social media. Don't provide private information online such as your address, phone number, credit card details or travel schedule (Fedor, 2022).



INFORMATIVE POSTER

Module : Digital skill
LCLM4002

EMILIA DELIU -2335587 GRP 2

Lecture : Dr . HOANG NGUYEN

Reference:

Fedor, O. (2022) *Internet Safety for College students*.

Available at: <https://www.findmysoft.com/cybersecurity/internet-safety-college-students/>(Accessed: 17 July 2024).

Smith, C . (2021) *Privacy and security* .

Available at: <https://itsnews.widener.edu/2021/10/07/cyber-security-awareness-month-phishing-awareness-tips/>(Accessed: 17 July 2024).

Chatzidrosos,K. (2024) *Security and privacy in the web through browser technology*.

Available at: <https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/30437/3307200004-1.pdf?sequence=1> (Accessed: 18 July 2024).