* BASIC DIGITAL SAFETY *

Module name: **Digital Skills**

Module code: **LCLM 4002_LON**

Student name: **Mario Massaro**

Student ID: **2335126**

Group: **5**

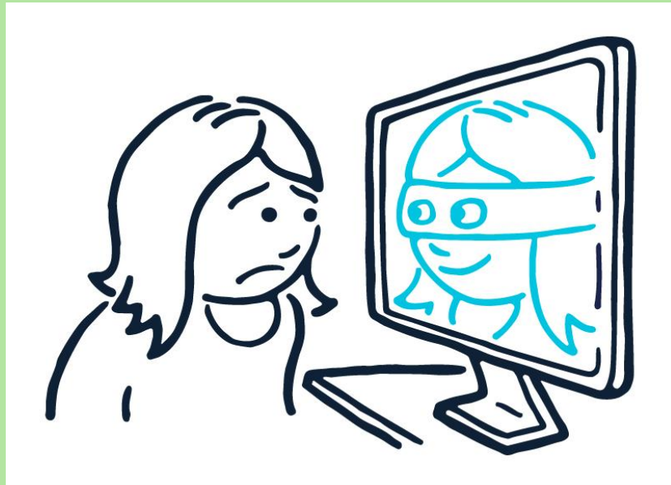
Lecture name: **Koushik Modak**

University: **University of Wales Trinity Saint David**

What the dangers are and how to protect yourself.

The modern Information Technology has revolutionized our life, our jobs, and relationship among the people, that technology helped us in many ways, both positive and negative.

There is no shadow of doubt about the multiple benefits that we obtain every day using modern technologies such as computer, laptop, tablet, smartphone, smart TV, smart car, and more. Nowadays it becomes increasingly unthinkable and unimaginable to live without these technological tools. They have become integral and fundamental parts in our daily life. The fact that all of these, for them to work at their best, must necessarily be connected to the internet. But at the same time, we are exposed to dangers such as violation of privacy, theft of personal and business data and details, banking details, personal identity, health details, for example: Phishing.



Phishing is a type of theft or robbery often associated with the cybersecurity industry. In phishing, just like a "fisherman", the phisher hooks and captures his victim by pretending to be a trusted person. The phisher's goal is to trick the victim into opening a malicious link or downloading a corrupted file to steal the desired information or irreparably damage devices. Protecting people, businesses, and organizations from a range of cyberthreats requires digital safety. Maintaining a secure and dependable online environment includes setting up and sticking to strong digital defence procedures. (NCSC, 2018).

Such as:

- Using a strong and different password for email and other accounts. Setting complicated access keys is an effective way to secure devices, data and online access.
- Turn on Two-Step Verification (2SV), or Two-factor authentication (2FA). This security method requires two types of identification to gain access, usually by giving a code to enter from an App or SMS.
- Back up of important documents, photos and other personal data to make sure that they can be recovered.
- Devices update (smartphones, laptops, tablets and computers), a security update set in automatic mode can provide greater protection for both devices and accounts.
- Have Critical Awareness to justify if the website is safety, by verifying at: https://check.getsafeonline.org.

Reference: National Cyber Security Centre, (2018). *Top tips for staying secure online.* Reviewed 2021/12/17. Available at: https://www.ncsc.gov.uk/collection/top-tips-staying-secure-online. [accessed: 22 July 2024]