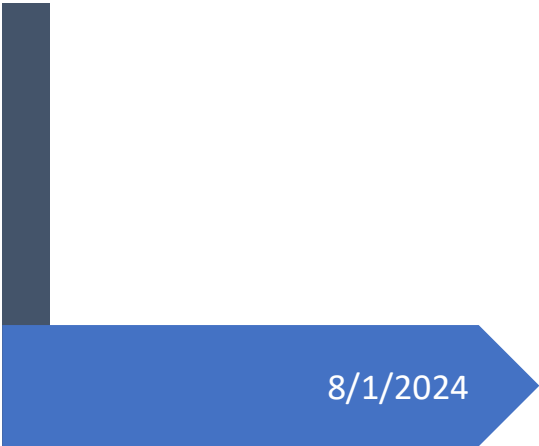


A dark blue vertical bar on the left side of the page. A blue arrow points to the right from the bar, containing the date 8/1/2024.

8/1/2024

Digital Safety

Module Name: Digital Skills

Module Code: LCLM4002

Student Name: Jemalyn Dela

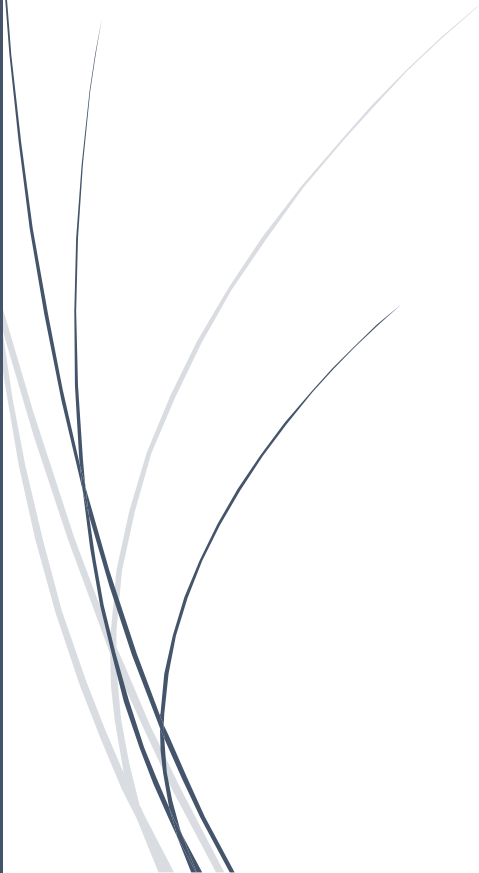
Student ID: 2355247

Group: 5

Lecturers Name: Amer Kareem

University of Wales Trinity Saint David

(London Campus)

Several thin, dark blue wavy lines originate from the bottom left corner and curve upwards and to the right, overlapping the vertical bar and the text area.



Poster

Digital safety is very important in the digital world to share information safely with others and save personal as well as business information from the hackers through taking necessary initiatives. More than half of total UK companies face cyberattack and 4,00,000 cases were filed for data breaching and fraud (Rademaker, 2019). As the cybercrime is increasing day by day, it is necessary to take initiatives in the workplace to ensure digital safety to protect information and the whole business.

Techniques to ensure digital safety

There are some ways to ensure digital safety such as 2 factor authentication, using strong password, backing up data, firewalls, PKI services, MDR services, antivirus software and so on (Rusdan, 2020). Executives and managers should focus on this issue to maintain strong security in the workplace. Companies should employ experts to ensure digital safety and reduce the chance of hacking that will reduce cost of the company and ensure safety of that company. Staff training is also important so that they can understand the importance of digital safety and don't do major mistakes that may violate safety and security in the workplace.

Challenges

Many employees and staffs don't have enough knowledge on digital technology that is a major challenge for companies to train them about digital technology and modern tools (Armstrong and Landers, 2019). There can be spam messages and phishing attack which are difficult to solve for small businesses. Internal stakeholders may often breach with the company and leak personal information.

Companies should invest in digital security and take help from experts to save the company from cyberattack because cyberattack can destroy a business (Fantin, 2010). From top executives to employees all should to learn about digital literacy and aware about the cyberattack so that they can maintain digital safety and ensure strong security in the workplace.

Reference

- Armstrong, M.B. and Landers, R.N. (2019). Gamification of employee training and development. *International Journal of Training and Development*, 22(2), pp.162–169.
- Fantin, M. (2010). Perspectives on Media Literacy, Digital Literacy and Information Literacy. *International Journal of Digital Literacy and Digital Competence*, 1(4), pp.10–15. doi:<https://doi.org/10.4018/jdlde.2010100102>.
- Rademaker, M. (2019). Assessing Cyber Security . *Information & Security: An International Journal*, 34, pp.93–104. doi:<https://doi.org/10.11610/isij.3407>.
- Rusdan, M. (2020). Designing of User Authentication Based on Multi-factor Authentication on Wireless Networks. *Journal of Advanced Research in Dynamical and Control Systems*, 12(1), pp.201–209. doi:<https://doi.org/10.5373/jardcs/v12i1/20201030>.