

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

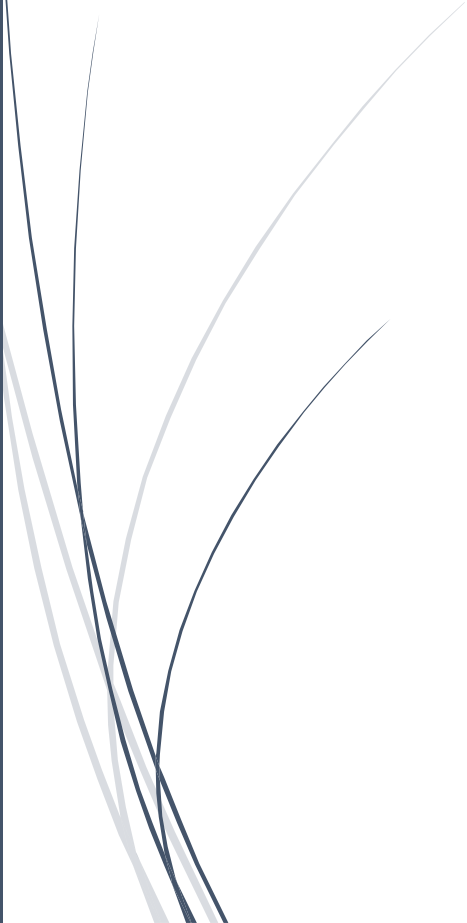
Student Name: Rahmia Sulay Kamil

Student ID: 2335591

Group: 6

Lecturers Name: Almotave Banik

University of Wales Trinity Saint David  
(London Campus)

Several thin, dark blue wavy lines that originate from the bottom left and curve upwards and to the right, resembling stylized grass or reeds.



## Digital Safety in the Workplace

Good morning, everyone. Today, we're discussing a critical topic: about digital safety in our place of work. The poster before you, outlines major measures to safeguard our company and yourself in the era of the online environment.

First, let's address passwords. The basis of digital security is establishing complicated and quite distinct passwords for various accounts. According to the National Institute of Standards and Technology, it is stated that "The length of the password is used as the main factor in determining password strength". Ideally, try to use 12+ characters including both the upper and lower case, numbers, and symbols.

Two factor authentication or 2FA, is another layer of security. This has to be enabled wherever possible, especially for email accounts. It is like having a double lock on your virtual gates or doors to your systems.

That is why phishing is still an issue of concern to this date. According to a Verizon report, "Phishing attacks accounted for 36% of data breaches" (Verizon, 2021). Stay vigilant: confirm the identity of the sender, do not open the links they suggest, and do not download the files that are sent by unknown people.

Maintenance is very important particularly when it comes to updating the software. These updates frequently fix security issues, which adds to the thickness of your shield against possible danger.

Smartphones play a central role in the lives of millions of people today and that is why protection of such devices is of paramount importance. Choose complex PINs, ensure your smartphone has the ability to wipe data remotely and do not use Wi-Fi connection in areas that are not secure for business related activities.

Cybersecurity is everyone's responsibility. Thus, by following these guidelines, we have a solid protection to prevent various digital threats. Our IT Security team is always ready to assist, feel free to contact us if you have any queries or issues.

We shall all play our part in ensuring that our workplace is safe when we are conducting our business online. I appreciate your attention and efforts towards the safety of the people.

## References

NIST, 2020. *Digital Identity Guidelines: Authentication and Lifecycle Management*. Gaithersburg, MD: National Institute of Standards and Technology, U.S. Department of Commerce. Available at: <https://pages.nist.gov/800-63-3/sp800-63b.html> [Accessed 30 July 2024].

Verizon, 2021. *2021 Data Breach Investigations Report*. Basking Ridge, NJ: Verizon Communications Inc. Available at: <https://www.verizon.com/business/resources/reports/dbir/> [Accessed 30 July 2024].