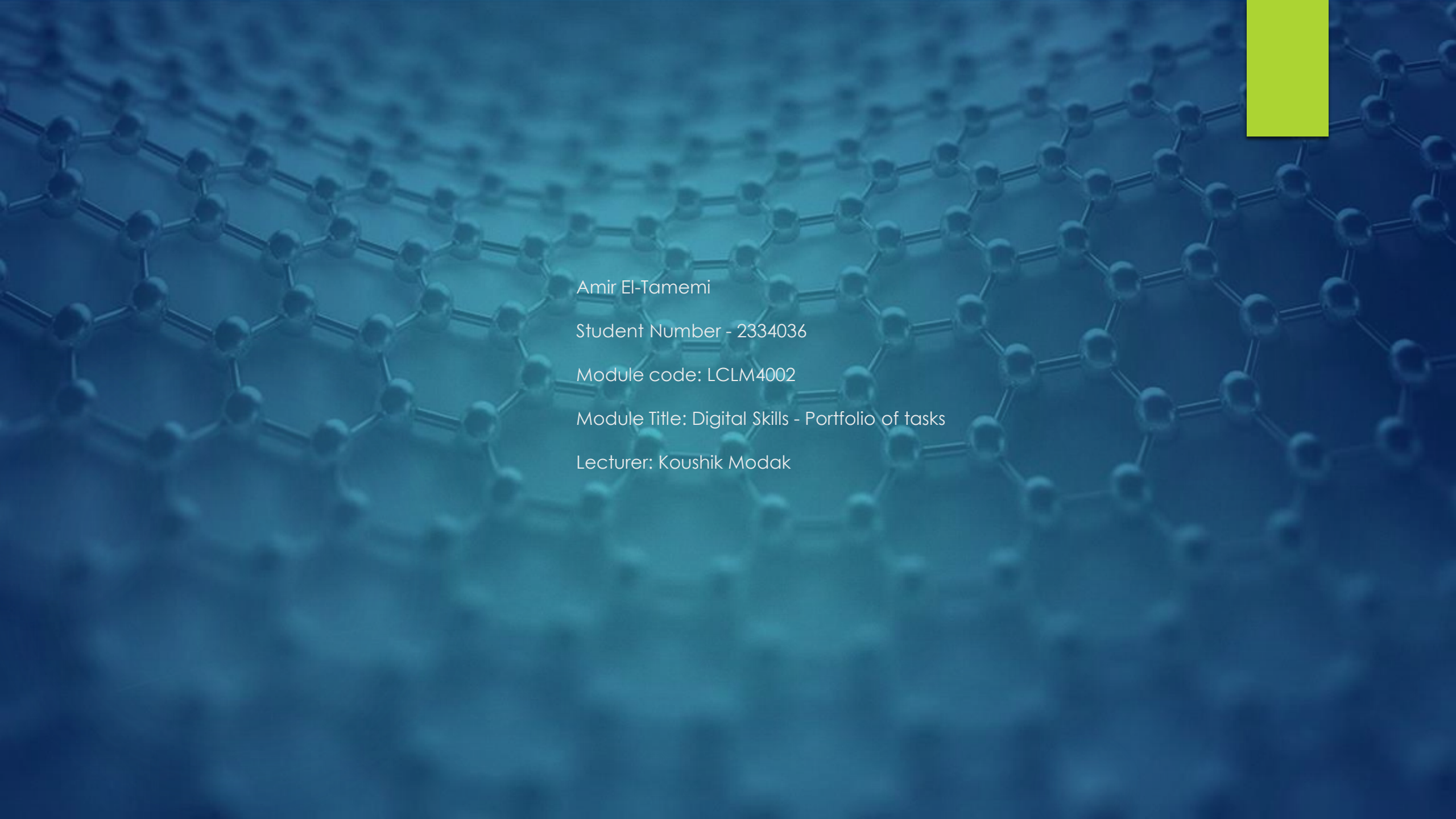




Amir El-Tamemi

Student Number - 2334036

Module code: LCLM4002

Module Title: Digital Skills - Portfolio of tasks

Lecturer: Koushik Modak



# Digital Safety



## Basic Digital Safety

Staying safe online in the modern day is crucial. Digital safety involves using practices and tools to protect our information and privacy.

### Password Security

Creating and managing strong passwords is a key part of digital safety. Florêncio and Herley (2007) state that passwords should be long, complex, and unique for each account to prevent unauthorised access. Many people use simple passwords or reuse the same one across different sites, which increases the risk of being hacked. It's best to use a mix of letters, numbers, and special characters. Password managers can help by storing and generating strong passwords (Sikorski, 2016).

### Recognising Phishing Attempts

Phishing is a method used by cybercriminals to trick people into giving away personal information like login details and credit card numbers. Knowing how to spot phishing attempts is vital for digital safety. Phishing emails often look real but have signs like generic greetings, urgent messages, and suspicious links or attachments (Jagatic et al., 2007). Users should be careful with unsolicited emails and avoid clicking on links or downloading attachments from unknown sources. Checking the sender's email address and looking for signs of fake emails can help identify phishing scams (Hong, 2012).



### Using Secure Networks

Using secure networks is another important part of digital safety, especially when accessing sensitive information. Public Wi-Fi networks are often insecure, making it easy for attackers to intercept data. Hlavacs et al. (2011) suggest avoiding sensitive activities on public networks or using virtual private networks (VPNs) to encrypt internet traffic. VPNs create a secure tunnel between the user's device and the internet, adding extra protection (Wu et al., 2016).

## Software Updates and Antivirus Protection

Keeping software up to date is crucial for digital safety. Software updates often fix security vulnerabilities that hackers could exploit (Arora et al., 2010). Users should enable automatic updates for their operating systems and apps to stay protected against the latest threats. Installing and regularly updating antivirus software also helps defend against malware, viruses, and other harmful programs (Morrow, 2012).



## Data Encryption and Backup

Encrypting data and regularly backing it up are essential for protecting information. Encryption turns data into code to prevent unauthorised access, ensuring that even if data is intercepted, it can't be read without the decryption key (Stallings, 2017). Regular backups ensure that if data is lost due to hardware failure, malware, or human error, it can be restored. Cloud services often provide encrypted backups, combining convenience with security (Ristenpart et al., 2010).

## Social Media Safety

With the widespread use of social media, it's important to follow safe practices to protect personal information. Users should be careful about what they share online, adjust privacy settings to limit visibility, and be wary of accepting friend requests from unknown individuals

(Boyd, 2007). Social media platforms are common targets for cyberattacks, and publicly shared information can be used for identity theft and other malicious activities.

## References

- Arora, A., Telang, R., & Xu, H. (2010). Optimal policy for software vulnerability disclosure. *Management Science*, 56(3), 434-449.
- Boyd, D. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. *MacArthur Foundation Series on Digital Learning–Youth, Identity, and Digital Media Volume*, 119-142.
- Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*, 657-666.
- Hlavacs, H., Treitl, S., & Weippl, E. (2011). On the security of public wireless LAN access. *Proceedings of the 7th International Conference on Network and Service Management*, 1-8.
- Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81.
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100.
- Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 2012(12), 5-8.
- Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2010). Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM conference on Computer and communications security*, 199-212.
- Sikorski, M. (2016). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press.
- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.
- Wu, T., Huang, S., & Ku, W. (2016). A VPN performance and security comparative evaluation in cloud computing environments. *Proceedings of the 2nd International Conference on Information Management and Security*, 1-6.