

## Task 1.

- 1- The threat of cybercrimes of phishing is real, but cybersecurity procedures are based on prevention assumption based on *cybersecurity D* course. to protect myself, I have taken several steps. After a phishing attempt, I enabled multi-factor authentication (MFA) on all my accounts and use a password manager for strong, unique passwords. Email filters block suspicious messages, and always verify links directly with organizations. My servers are secured with updates, firewalls, and intrusion detection systems (IDS), and I remove all my payment details or bank cards from my email account and use secure payment method. I also stay informed on phishing tactics by following on social media the phishing crimes and how they are do it, also reading the warning letter from the authorities.
  
- 2- I encountered a phishing attempt where an attacker pretended to be an official authority, asking to update my personal information through a phishing link, the email looked convincing with official logos and formal language. I did not fall for it but I realized how easy it is to get hacked.  
Actions to improve: improve email security filters, regularly check account activity for any signs of compromise.