Exercise 3.task2

1- Because phishing attacks can take advantage of emotional reactions and cognitive biases in humans, they are very successful. Attackers frequently utilize power, fear, and hurry to force victims to act without giving their actions any thought. Phishing emails, for instance, might pose as reliable organizations (like banks) and incite panic by stating that accounts are compromised in order to trick users into opening dangerous links. These psychological ploys take advantage of cognitive shortcuts, which cause people to react hastily to imagined emergencies rather than thoroughly assessing the circumstances (Trellix, Ridge Security). Phishing is appealing to attackers because it is scalable and simple to implement (Cyber-Ed).

2- Because it takes advantage of behavioral psychology and innate human traits like helpfulness and faith in authority, social engineering is effective. Attackers deceive people by pretending to be reputable individuals (such as CEOs or IT staff) or fabricating believable scenarios that make it difficult for victims to refuse. Pretexting and baiting are two strategies that take use of people's authority and reciprocity biases to get them to reveal private information when under social pressure. Strong emotional triggers that impair judgment include fear, curiosity, and urgency (PhishTrap Blogs; Cyber-Ed). Social engineers take advantage of security systems by focusing on human vulnerability and feeding on these inclinations.
3- Remembering complicated, one-of-a-kind passwords for numerous accounts is a cognitive burden that causes many people to struggle with password security. According to behavioral psychology, people are more likely to choose short, memorable passwords or to use the same one across many platforms since they are more convenient. Furthermore, users may underestimate the hazards associated with using bad password practices because they are not always immediately apparent, which encourages unsafe behavior (Trellix). Reusing passwords is one example of an insecure action that doesn't immediately result in feedback, which reinforces bad habits.

4- Though theoretically solid, PGP (Pretty Good Privacy) has significant usability issues, particularly for non-technical users. According to cognitive psychology, the typical user cannot handle encryption keys or decipher the subtleties of email encryption. PGP's methods are hard to learn and keep up with, which deters mass adoption. The tool's usefulness as a mass-market solution is undermined by behavioral factors such as ease and the perceived complexity of the tool, which lead users to favor simpler and less secure ways. Furthermore, it's possible that people are unaware of the benefits of encryption in regular contact (Cyber-Ed).

5- Because malware authors take advantage of both technological flaws and human tendencies, it spreads quickly. The belief that users have in well-known businesses or social networks is the foundation for phishing emails, malware downloads, and compromised websites. Users who fall victim to cognitive biases such as optimism bias (the conviction that "it won't happen to me") disregard security alerts and click on dubious websites. Moreover, contemporary malware is engineered to be extremely contagious, taking advantage of user carelessness and software flaws to spread swiftly across networks (PhishTrap Blogs; Ridge Security). By preying on people's interest and trust, social engineering techniques like baiting and pretexting let malware spread farther (PhishFirewall).