RISKS IN NETWORKING TECHNOLOGY

1.Malware – These are software made to cause damage to a computer,server,client or network,gain classified information and prevent access of information.

2.Phishing – A fraud of sending messages pretending to be from a known organization in order to get users to give out personal information such as passwords in order to use them for performing vices such as theft.

3.Ransomware – A type of malicious software that prevents users from accessing the system until a specified ransom demand is met . Some use cryptoviral extortion which could damage the files locked.

4. Computer virus – A program that infects some areas of a computer,replicates itself by modifying other computer programs and inserting its own code into those programs.

5.DDoS(Distributed Denial-of-Service) – This involves flooding a server with internet traffic to prevent users accessing online sites and services.

6.Drive-by Download – An unintentional download of malicious code to a computer or mobile device,exposing the victim to a cyber-attack.

7.DNS attack - Occurs when a threat actor exploits vulnerabilities in a domain name system.

8.Insider threat – A perceived threat to an organization from people within the organization who have inside information about its security practices,data and computer systems.

9.SQL Injection – A common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

10.Man-in-the-middle attack – A cyberattack where the attacker gets in the middle of two unknowing parties to intercept their communications and data for devious intentions such as hacking.

references

www.imperva.com

www.fortinet.com

www.trendmicro.com

www.wikipedia.com