Security features protect against unauthorized access and cyber threats/attacks to the system. Forms of accidental and malicious security violations: Breach of confidentiality, theft of information, breach of integrity, unauthorized modification of data, breach of availability unauthorized destruction of data, theft of service, unauthorized use of resources, denial of service, preventing legitimate use of the system

To protect the system, there are four levels of security measures: Physical, securing the machine room, terminals, and workstations; Human, providing access only to appropriate users access to the system; and Operating System: the system itself needs to be protected from accidental or purposeful security breaches; network: the lines in which the system data travels through private lines, shared lines like the Internet, wireless connections, or dial-up lines.

Program threats: Back-door provides information or allows easy access, Trojan horse: a code segment that misuses its environment, Spyware: another variation of trojan horse sometimes accompanies a program that the user has chosen to install which creates pop-up browser windows when particular sites are visited, Virus: a fragment of code embedded to “infect” other programs, Worms: process that uses spawns copies of itself to reproduce themselves among systems and thus shut down an entire network.

Security tools: Cryptography is used to constrain a message's potential senders and/or receivers. Encryption is a means of constraining the possible receivers of a message Multifactor Authentication (MFA) username and password. Still, you are asked to provide a one-time access code that the website sends to the user’s cell phone or email address.