Quizlet

FIT2090 - W12

Leave the first rating

STUDY

- Flashcards
- Learn
- Write
- Spell
- Test

PLAY

- Match
- Gravity
- Live BETA

mrcobbl

Key concepts:

Antivirus Software | Security Policy | Computer Networks

Terms in this set (21)

Ransomware	Software that encrypts programs and data until a ransom is paid to remove it.

Viruses	A piece of programming code (usually disguised as something else) that causes a computer to behave in an unexpected and undesirable manner
Worms	A harmful program that resides in the active memory of the computer and duplicates itself - Can propagate without human intervention
Trojan Horse	a program that appears desirable but actually contains something harmful duplicates itself
blended threat	a security threat that combines the characteristics of computer viruses, worms, and other malicious codes with vulnerabilities found on public and private networks
Spam	unwanted e-mail (usually of a commercial nature sent out in bulk)
Distributed Denial-of-Service Attacks (DDOS)	An attack in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks
Rootkit	program that hides in a computer and allows someone from a remote location to take full control of the computer
Advanced Persistent Threat	a sophisticated, possibly long-running computer hack that is perpetrated by large, well-funded organizations such as

	governments
Phishing	An attack that sends an email or displays a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information
Smishing and Vishing	Smishing is a variation of phishing that involves the use of texting Vishing is similar to smishing except the victims receive a voice mail message telling them to call a phone number or access a Web site
Cyberespionage	efforts by intelligence agencies to penetrate computer networks of an enemy nation in order to steal important data
Cyberterrorism	politically motivated attacks on information systems
A strong security program begins by	Assessing threats to the organization's computers and network Identifying actions that address the most serious vulnerabilities Educating users about the risks involved and the actions they must take to prevent a security incident
security policy	Defines an organization's security requirements along with the controls and sanctions needed to meet those

	requirements Outlines what needs to be done but not how to do it Automated system rules should mirror an organization's written policies
Educating Employees and Contract Workers	Guarding their passwords to protect against unauthorized access to their accounts Prohibiting others from using their passwords Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction
Firewall	a part of a computer system or network that is designed to block unauthorized access while permitting outward communication.
Next-generation firewall (NGFW)	A firewall that combines firewall software with anti-malware software and other software that protects resources on a network.
antivirus software	scans and searches hard drives to prevent, detect, and remove known viruses, adware, and spyware
Another safeguard	Create roles and user accounts so that users have the authority to perform their responsibilities and nothing more
security audit	comprehensive review of organizational security