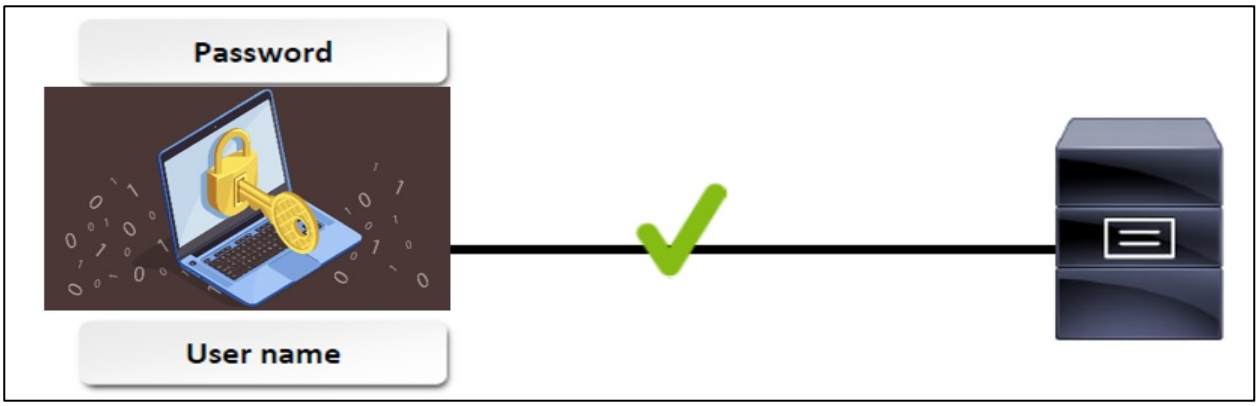
Lec 10: Protection
Dr. Sedeeq Al-khazraji
2024-2025

Safeguards against Computer Malware

Methods that guarantee a computer or network is safe from the different malicious software simply do not exist. User can take several precautions, however, to protect their personal and work computers from these malware infections.

1. Strong password protects your account

A password is a private combination of characters associated with the username that allows access to certain computer resources.



- **Create a password with adequate length**
  - They should never be less than eight characters and preferably longer. Short passwords can easily be determined by a brute-force password cracker.
- **Adequate character mix**
  - A good policy is to use a meaningless combination of letters and numbers that is seven or eight characters long.
- **Avoid using directly identifiable information**
  - They should not be the names of family members or pets or anything else that would be easy for a hacker

- Examples of weak passwords: “orange”, “97435333”, “alabri”
- Examples of strong passwords: “OraNge@3241”, “Al#Abri@4429”

2. Backup and Recovery

Backup is a way to copy or back up, selected files or an entire hard disk to another storage medium such as another hard disk, optical disc, USB flash drive, or tape. This method allows users to prevent data loss caused by system failure or hardware/software/information theft.

3. Regular updating software

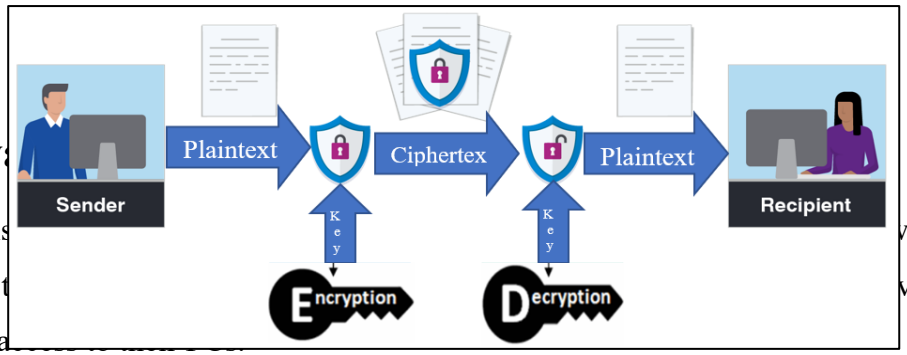
- **Security update**
  - Designed to protect your software (and computer) from harmful programs, viruses, and exploits
- **Updating applications**
  - Additions to software that can help prevent or fix problems, or enhance and improve how your computer works.
- **Update operating system applications**
  - Enhanced overall performance of the software and the computer is also often a good reason to keep up-to-date with updates to your PC programs

4. Digital certificates

A digital certificate is a notice that guarantees a user or a Web site is legitimate. Web browsers, such as Internet Explorer, often display a warning message if a Web site does not have a valid digital certificate.

5. Encryption and Decryption

Encryption is a security technique that converts readable data (plaintext form) into unreadable characters (cipher text form) to prevent unauthorized access. Decryption is the inverse process of encryption that allows only authorized parties with the necessary decryption information to read the encrypted files.



6. Priv

Privacy is vser tracking, and access to t vior of individuals or to get a

7. Firewall

A firewall is hardware and/or software that protects a network's resources from intrusion by users on another network such as the Internet. It filters and controls the traffic flow of information coming into and out of a network to decide which traffic to allow access to and which traffic to block. Organizations use firewalls to protect network resources from outsiders and to restrict employees' access to sensitive data such as payroll or personnel records.

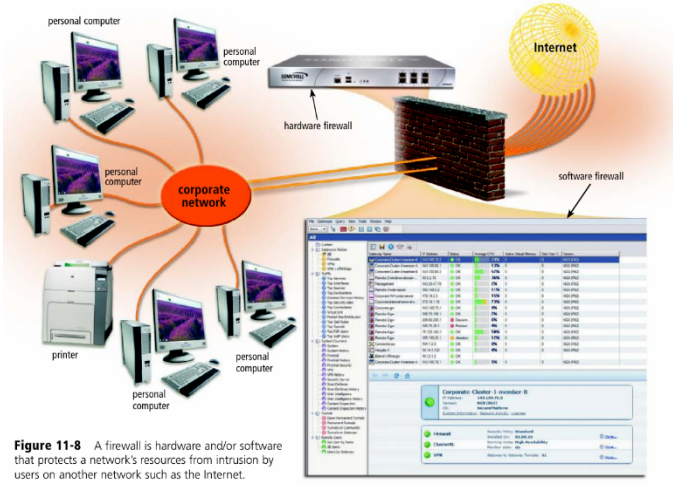


Figure 11-8 A firewall is hardware and/or software that protects a network's resources from intrusion by users on another network such as the Internet.

8. Antivirus Software

An antivirus program is a type of utility program used to protect a computer against viruses by scanning and removing any computer viruses found in memory, on storage device, or on incoming files. Most antivirus software has the capability also to protect against worms, Trojans and spyware.

Popular Antivirus Programs

- AVG Anti-Virus
- avast! antivirus
- CA Anti-Virus
- F-Secure Anti-Virus
- Kaspersky Anti-Virus
- McAfee VirusScan
- Norton AntiVirus
- Trend Micro AntiVirus
- Vexira AntiVirus