

FIVE BASIC IT SECURITY STEPS

Operating system updates. No software is bug-free. Hackers exploit loopholes for a variety of reasons, and it is critical that software be updated on a regular basis. Most operating systems, firewalls, and antivirus software include an automatic online update feature.

Firewalls. Firewalls separate one network from another. They are frequently used to separate a provider's internal network from the Internet. Firewalls not only hide the identity of individual computers, they also examine and filter potentially damaging data entering or leaving the network.

Antivirus protection. Hundreds, if not thousands, of new malicious software programs—viruses, worms, and so forth—are released each month. Because viruses can slip through firewalls by posing as a legitimate e-mail or program, installation of antivirus software on individual PCs is important.

Periodic backups. Periodic backups are required to ensure business continuity in case of an accident, such as a hard-drive failure or security attack. Data backups to an external hard drive or CD-ROM should occur at least once a week, and the backup data should be securely stored off-site. Backup processes should be tested to ensure that data can be restored in case of an operational failure.

Strong passwords. Passwords authenticate the identity of an individual user. Unless otherwise protected, sensitive data is exposed whenever a password is broken. Poorly chosen passwords can be uncovered in a matter of minutes with basic software. Good password security requires a combination of upper and lower-case letters; numbers; and symbols.