

Basic Computer Security Tips for Small Business

Fact Sheet – Crime Prevention

Is your business' computer system safe? Could an intruder sneak in and steal your information, or plant a virus? A common problem caused by computer viruses has been extensive damage to files, software, and operating systems that leave the user with a blank screen and costly repair bills. Often, more importantly, the business may lose irreplaceable data, such as customer and financial records. The following are seven essential steps a small business should take to secure its computer system.

Use Strong Passwords

Choose passwords that are difficult or impossible to guess. Give different passwords to all accounts. Use a combination of upper and lower case letters and numbers for passwords.

Back-up Critical Data

Make regular backups of critical data. Backups must be made at least once each day. Larger organizations should perform a full backup at least weekly, and incremental backups every day. At least once a month, the backup media should be verified.

Use Virus Protection Software

Install virus protection software on your computer, and update it daily for new virus signature updates. Scan all the files on your computer periodically.

Install Firewalls

Use a firewall as a gatekeeper between your computer and the Internet. Firewalls are usually software products. They are essential for those who keep their computers online through the popular DSL and cable modem connections, but they are also valuable for those who still dial in.

Avoid Unnecessary Connections

Do not keep computers online when not in use. Either shut them off or physically disconnect them from an Internet connection.

Monitor E-mail

Do not open e-mail attachments from strangers, regardless of how enticing the "subject line" or attachment may be. Be suspicious of any unexpected e-mail attachment from someone you do know as it may have been sent from an infected machine without that person's knowledge.

Keep Operating Systems Current

Many commonly-used operating systems, as well as other programs, such as Web browsers and e-mail readers, have security holes or flaws. The software companies regularly issue fixes, called "patches." Keep your operating system up-to-date by regularly downloading these security patches from the software vendor's Web site.