Computer Security Tips for Small Business

Is your business' computer system safe? Could an intruder sneak in and steal critical 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. Or, as 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.

Backup 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 backup 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 cable modem connections, and they are just as valuable for those who still dial in. Compartmentalize information within the company, too. Limit access to key areas, such as financial data, proprietary information, and customer portals

Avoid Unnecessary Connections

Do not keep computers online when not in use. Either shut them off or physically disconnect them from an internet connection. Hackers can compromise a system if certain ports are left vulnerable. Vulnerabilities that provide remote hackers full file-system read and write capabilities, remote execution of commands as a root, or administrator user could occur.

Monitor Email

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

Keep Software and Operating System Current

Many commonly-used operating systems, as well as other programs, such as web browsers and email 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 website.

Screen Employees

Do background checks, and get at least two references for all new employees. Ask for at least two references from previous employers and call them to verify previous employment information. You may also want to check if a prospective employee has a criminal record or a problem with his credit history.