Ten Cybersecurity Strategies for Small Businesses

Broadband and information technology are powerful factors in small businesses reaching new markets and increasing productivity and efficiency. However, businesses need a cybersecurity strategy to protect their own business, their customers, and their data from growing cybersecurity threats.

1. Train employees in security principles
Establish basic security practices to protect sensitive business information and communicate them to all employees on a regular basis. Establish rules of behavior describing how to handle and protect customer information and other vital data. Clearly spell out the penalties for violating business policies.

2. Protect information, computers and networks from viruses, spyware and other malicious code
Install, use and regularly update antivirus and antispyware software on every computer used in your business. Such software is readily available online from a variety of vendors. Most software packages now offer subscriptions to "security service" applications, which provide additional layers of protection. Set the antivirus software to automatically check for updates at a scheduled time of low computer usage, such as at night (midnight, for example), and then set the software to do a scan after the software update.

3. Provide firewall security for your Internet connection
A firewall is set of related programs that prevent outsiders from accessing data on a private network. Install and maintain firewalls between your internal network and the Internet. If employees work from home, ensure that their home systems are protected by firewalls. Install firewalls on all computers – including laptops – used in conducting your business.

4. **Download and install software updates for your operating systems and applications as they become available**
All operating system vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install such updates automatically.

5. Make backup copies of important business data and information.
Regularly backup the data on every computer used in your business. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounts receivable/payable files. Backup data automatically if possible, or at least weekly.

6. Control physical access to your computers and network components
Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft, so make sure they are stored and locked up when unattended.

7. Secure your Wi-Fi networks
If you have a Wi-Fi network for your workplace make sure it is secure and hidden. To hide your Wi-Fi network, set-up your wireless access point or router so it does not broadcast the network name also known as the Service Set Identifier (SSID). In addition, make sure to turn on the encryption so that passwords are required for access. Lastly, it is critical to change the administrative password that was on the device when it was first purchased.

8. Require individual user accounts for each employee
Setup a separate account for each individual and require that strong passwords be used for each account. Administrative privileges should only be given to trusted IT staff and key personnel.

9. Limit employee access to data and information, and limit authority to install software
Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10. Regularly change passwords
Passwords that stay the same, will, over time, be shared and become common knowledge to coworkers and can be easily hacked. Passwords should be changed at least every three months.

The FCC's Cybersecurity Hub at www.fcc.gov/cyberforsmallbiz has more information, including links to free and low-cost security tools.