

Wellspring Info

10 Cybersecurity Tips from the FCC



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 and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

2. Protect information, computers and networks from cyber attacks

Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. Provide firewall security for your Internet connection

A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4. Create a mobile device action plan

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5. Make backup copies of important business data and information

Regularly backup the data on all computers. 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 and store the copies either offsite or in the cloud.

6. Control physical access to your computers and create user accounts for each employee

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel

7. Secure your Wi-Fi networks

If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. Employ best practices on payment cards

Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

9. Limit employee access to data and information, 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. Passwords and authentication

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Wellspring Info can improve your emergency response plan, boost your OSHA-compliance, and then turn your plan into emergency guidebooks or an app:

Guidebooks: www.WellspringInfo.com

App: www.WellspringInfoApp.com

Phone: 800.268.3682

Terms & Conditions of Wellspring Info, Inc.'s content suggestions: Any content or content suggestions provided by Wellspring Info are provided "as is" without representation or warranty of fitness for a particular purpose. The risk as to the quality, accuracy, and performance of the content is with you. You agree to indemnify, defend and hold Wellspring Info, Inc., its affiliates, employees, shareholders, partners, vendors, and content sources harmless from and against any and all claims, liability, losses, damages, costs and expenses.