

12 CYBER SECURITY TIPS FOR SMALL BUSINESSES

Maintaining strong cybersecurity habits is crucial to the security of your business. Here are 12 tips from the FCC you can take to protect your livelihood.



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. Conduct cybersecurity training annually and share information via internal channels regularly.



Protect Information, Computers, and Networks from Cyber Attacks

Keep your machines clean: 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.



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.



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.



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.



www.texasfirst.bank ★ Member FDIC



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. Establish a process to deactivate terminated employees and users immediately.



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.



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.



Limit Employee and Third-Party Vendor Access to Data And Information, Limit Authority to Install Software

Do not provide any one employee or vendor with access to all data systems. Employees and third-party vendors 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.



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.



Vendor Management

Establish a procedure to vet third-party vendors for cybersecurity compliance. Limit their access to necessary systems only and require signed data protection agreements. Monitor vendor security and audit their permissions regularly.



Incident Response and Recovery

Maintain an incident response plan. Document all incidents and notify internal and external stakeholders as needed. Identify experts and legal counsel in advance and engage if necessary. Conduct post-incident reviews immediately after an incident and update protocols.

To learn more about tips to protect your business, visit our Security Center:

www.texasfirst.bank/security-center



www.texasfirst.bank ★ Member FDIC