**CYBERSECURITY TIPS FOR SMALL BUSINESSES**

From: Lana M. Glovach, U.S. Small Business Administration ([SBA](https://www.sba.gov/))

Is your small business prepared for a cybersecurity breach? Small businesses increasingly rely on information technology to store, process, and communicate information, and they have valuable information cybercriminals seek, including employee and customer data, bank account information and access to the business's finances, and intellectual property. Small businesses also provide access to larger networks such as supply chains. Protecting this information against increasing cyber threats is critical. As we learn almost every day from the news, data breaches can have significant negative impacts – financial and reputational – on a business, especially a small business. The information and resources provided in this article is designed to help small businesses better protect the data of their customers, employees, and business partners.

*Top Ten Security Tips*

1. **Protect against viruses, spyware, and other malicious code**
Make sure each of your business’s computers is equipped with antivirus software and antispyware, and update them regularly. Such software is readily available online from a variety of vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.
2. **Secure your networks**
Safeguard your Internet connection by using a firewall and encrypting information.  If you have a Wi-Fi network, 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, known as the Service Set Identifier (SSID). Also password protect access to the router.
3. **Establish security practices and policies to protect sensitive information**
Establish policies on how employees should handle and protect personally identifiable information (PII) and other sensitive data.  Clearly outline the consequences of violating your business’s cybersecurity policies.
4. **Educate employees about cyber threats and hold them accountable**
Educate your employees about online threats and how to protect your business’s data, including the safe use of social networking sites.  Depending on the nature of your business, employees might be introducing competitors to sensitive details about your firm’s internal business. Employees should be informed about how to post online in a way that does not reveal any trade secrets to the public or competing businesses.  Hold employees accountable to the business’s Internet security policies and procedures.
5. **Require employees to use strong passwords and to change them often**
Consider implementing multifactor 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 multifactor authentication for your account.
6. **Employ best practices on payment cards**
Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor. Isolate payment systems from other, less secure programs, and do not use the same computer to process payments and surf the Internet.
7. **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 on the cloud.
8. **Control physical access to computers and network components**
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.
9. **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 establish reporting procedures for lost or stolen equipment.
10. **Protect all pages on your public-facing websites, not just the checkout and sign-up pages**

***Source***: [FCC’s Cybersecurity Tips for Small Businesses](https://www.fcc.gov/general/cybersecurity-small-business) and [DHS’s Small Business Tip Card](https://www.dhs.gov/sites/default/files/publications/Small-Business-Tip-Card_04.07.pdf)

The SBA wants to help your small business plan for success. To learn more about the SBA’s programs and services, please contact Lana Glovach, SBA Economic Development Specialist, at lana.glovach@sba.gov or 401-528-4575. Assistance is available in languages other than English, including Spanish, and all SBA programs and services are extended to the public on a non-discriminatory basis.