10 TIPS

CALIFORNIA SBDC | Small Business Development Centers
www.californiasbdc.org

TO COMPUTER SECURITY FOR YOUR SMALL BUSINESS

California Small Business Development Center Network

You've got questions.
We've got answers.

www.californiasbdc.org

As small businesses become more reliant on technology, they also become more vulnerable to cybercrime. A Gartner study found that 90 percent of companies that suffer major data loss close within two years—but that 80 percent of business owners have no plan to protect their data. Here are 10 tips to secure your business's computers.

1. **Identify security needs and risks.** Inventory your computer equipment, data and potential risks. Who is using desktops, laptops, tablets or smartphones? Where and how are they being used? What data do you collect, store or share, and who can access it? If your computers or network security were breached, how would extended downtime, fines or lawsuits affect your company? A Symantec study found cyber-attacks cost small and midsized businesses an average of $188,242, with downtime costing $12,500 a day.
2. **Begin with the basics.** Set up company computers and devices with strong passwords, and change them regularly. Ensure computers and devices are protected by antivirus, antispam and antispyware software; intrusion prevention systems; encryption technology to protect email traffic and wireless networks; and firewalls. AVG, BitDefender, McAfee, Norton, Symantec and Trend Micro offer popular security products.
3. **Keep your systems updated.** Software updates often fix security problems, so download updates as soon as they become available. To make this easier, more software programs--including Windows, Office, Flash, Java and Adobe Acrobat—now offer options to download and install updates automatically; these can generally be accessed through "Settings" or "Preferences."
4. **Back up.** There's no excuse not to back up data when today's online backup solutions run unobtrusively in the background and store information safely offsite. BackBlaze, Carbonite, Mozy and SpiderOak are popular online backup services for small businesses. Ask about file sharing and sync across multiple devices and users, how much storage you get, how easy it is to restore data, and what backup and disaster plans the backup company itself has in place. Double your protection by backing up to external hard drives in your office.
5. **Educate employees.** Even with the right systems in place, your business is still vulnerable to human error. Educate employees about the importance of using strong passwords and protecting them. Explain the risks of opening texts or attachments from unknown senders, clicking on suspicious links in emails, or sharing too much company information on social networks.
6. **Think mobile.** If your employees use mobile devices for business, install updated security technology, encrypt data and use virtual private networks (VPNs) to enable secure remote access. Remind employees to be cautious about who may be watching when they enter passwords or view confidential data outside the office.
7. **Keep devices safe.** While viruses and hackers capture headlines, the loss or theft of a physical device is still the most common cause of data breaches, according to Symantec. Remind mobile employees to be aware of their surroundings and never leave company laptops, tablets or cellphones exposed in a vehicle or unattended. Have them immediately report lost or stolen devices.
8. **Don't mix business and family.** Working on the same computer your children use for games or email puts business data at risk. Employees who work at home might have valuable work data on family computers. Create rules for how data can be shared or, if employees use company computers to work at home, consider restricting access to certain websites or prohibiting use of those computers for personal business.
9. **Secure your site.** Symantec reports 90 percent of consumers will leave your site if they get the warning "This site is not secure." Privacy and security seals show customers your website is a safe place to browse or shop. Privacy seals verify your privacy protection policy; security seals verify that you use technology such as encryption and regular scans for malware. McAfee, Norton, Symantec and TRUSTe are among providers offering these seals.
10. **Get expert help.** If you don't have an IT person on staff, enlist an IT consultant or SBDC Business Advisor to help you create a computer security policy. The SBA offers a series of free computer security workshops for small business owners, and the FCC has a customizable Small Business Cyber Planner.

By Rieva Lesonsky

Rieva Lesonsky is founder and President of GrowBiz Media, a media company that helps entrepreneurs start and grow their businesses. Before launching her business, she was Editorial Director of Entrepreneur *Magazine. Follow Rieva at Twitter.com/Rieva, and visit her website, SmallBizDaily.com, to get the scoop on business trends and sign up for free TrendCast reports.*

U.S. Small Business Administration SBA Your Small Business Resource

The Small Business Development Centers are funded by the U.S. Small Business Administration, host institutions of lead and service centers, state and local funds, and corporate partners. Funding is not an endorsement of any product, opinion, or service. All Federal and State funded programs are extended to the public on a nondiscriminatory basis. Special arrangements for individuals with disability will be made if requested in advance.