McAfee® for Consumer

McAfee Security Advice Center

Online Safety Tips

Any time you connect to the Internet you are vulnerable to cyber attacks. Hackers can steal your credit card numbers, tax records and passwords, or even completely disable your PC. Follow these tips to help avoid problems:

1. **Create smart and strong passwords.** Make it difficult for hackers to crack your password. You can create a smart password by incorporating capital letters, numbers, and special characters, and using more than six characters. An example of a strong password is: *Go1dM!n3*.
2. **Use email wisely.** Email is a great way to keep in touch with friends and family, and as a tool to conduct business. Even if you have good security software on your PC, however, your friends and family might not have the same protection. Be careful about what information you submit via email. Never send your credit-card information, Social Security number, or other private information via email.
3. **Be smart when using instant messaging (IM) programs.** If you use an IM program to communicate with friends and family, be careful about sending any personal information through online communications. Protect yourself by using a nickname for your IM screen name, so your name isn't identified through IM. Never accept strangers into your IM groups. Be smart about how you use IM at work because your employer has the right to monitor and view your messages.
4. **Shop safely.** If you plan to order from an online store, be sure that the Web site uses secure technology. When you are at the checkout screen, verify that the Web address begins with *https.* Also, check to see if a tiny locked padlock symbol appears at the bottom right of the checkout screen, or that there is a statement on the checkout screen stating that the pages are secure with a security technology vendor. Check that the security technology does exist by checking the security technology company's web site.
5. **Watch out for phishing scams.** Phishing scams use fraudulent emails and fake web sites, masquerading as legitimate businesses, to lure unsuspecting users into revealing private account or login information. To be safe, if you receive an email from a business that includes a link to a web site, make certain that the web site you visit is legitimate. Instead of clicking through to the site from within the email, open a separate Web browser and visit the business' web site directly to perform the necessary actions. You can also verify that an email is in fact from a legitimate business by calling the business or agency directly.
6. **Fun and carefree online gaming.** Internet games are fun for the whole family. Make sure you are careful when playing online games, especially when communicating with other players. Be sure that your security software still functions when you are in gaming mode.
7. **Pay attention to your children's online activities.** Keep your home computer in a community area so that you can monitor their activity. Use child software that is age-appropriate. Limit your children's time spent online. Install and use parental controls software that allows you to monitor your children's activity online. This will keep your children from accessing undesirable Web sites and sharing personal information via online communications.
8. **Subscribe to McAfee computer security service.** Keeping you and your family safe whenever you power on your computer, McAfee's comprehensive security software is always active—updating and protecting wherever you go online. McAfee products offer the latest and best combination of software, providing consumers and their home computers with unparalleled, comprehensive protection from cyberspace threats like viruses, spyware, adware, spam and identity theft.

We accept: VISA MasterCard DISCOVER AMERICAN EXPRESS PayPal

© 2003-2017 McAfee, LLC