

McAfee Security Tips

13 Ways to Protect Your System

In addition to installing our products, we recommend that you follow these simple, common-sense precautions to reduce your exposure and protect your system.

1. **Do not open e-mail attachments from an unknown, suspicious, or untrustworthy source.** If you're not familiar with the sender, do not open, download, or execute any files or e-mail attachments.
2. **Do not open an e-mail attachment unless you know what it is, even if it appears to come from a friend or someone you know.** Some viruses replicate themselves and spread via e-mail. Stay on the safe side and confirm that the attachment was sent from a trusted source before you open it.
3. **Do not open any e-mail attachments if the subject line is questionable.** If you feel that the attachment may be important to you, always save the file to your hard drive before you open it.
4. **Delete chain e-mails and other spam from your inbox.** It's best not to forward or reply to messages like these. Unsolicited, intrusive mail clogs up networks, may contain annoying or offensive content, and may result in security and privacy risks.
5. **Exercise caution when downloading files from the Internet.** Make sure that the Web site is legitimate and reputable. Verify that an anti-virus program has checked the files on the download site. If you have any doubts, don't download the file at all. If you download software from the Internet, be especially vigilant of free software, which often carries adware or other potentially unwanted content along with it. Always read the privacy policies and end-user license agreements (EULAs) for software you install, regardless of the source. Be especially wary of screensavers, games, browser add-ons, peer-to-peer (P2P) clients, and any downloads claiming to be "cracked" or free versions of expensive applications, such as Adobe® PhotoShop® or Microsoft® Office. If it sounds too good to be true, it probably is.
6. **Avoid downloads from non-Web sources altogether.** The chances of downloading infected software from Usenet groups, IRC channels, instant messaging clients, or P2P is very high. Links to Web sites seen in IRC and instant messaging also frequently point to infected downloads. Avoid obtaining your software from these sources.
7. **Update your anti-virus software often.** Threats are on the increase, and they are constantly evolving. Hundreds of viruses are discovered each month. To make sure that you are protected against the newest breed of threats, update your anti-virus software frequently. That means downloading the latest virus signature files and the most current version of the scanning engine.
8. **Back up your files frequently.** If a virus infects your files, at least you can replace them with your back-up copy. It's a good idea to store your backup files (on CDs or flash drives) in another secure physical location away from your computer.

9. **Update your operating system, Web browser, and e-mail program on a regular basis.** For example, you can get Microsoft® security updates for Microsoft® Windows® and Microsoft® Explorer at <http://www.microsoft.com/security>.
10. **Vigilance is the best defense against phishing scams.** “Phishing” describes scams that attempt to acquire confidential information such as credit card numbers, personal identity data, and passwords by sending out e-mails that look like they come from real companies or trusted individuals. If you happen to receive an e-mail message announcing that your account will be closed, that you need to confirm an order, or that you need to verify your billing information, do not reply to the e-mail or click on any links. If you want to find out whether the e-mail is legitimate, you can contact the company or individual directly by calling or writing to them.
11. **Do not open messages or click on links from unknown users in your instant messaging program.** Instant messaging can be a vehicle for transmitting viruses and other malicious code, and it’s another means of initiating phishing scams.
12. **Use a personal firewall.** A hardware firewall that sits between your DSL router or cable modem will protect you from inbound attacks. It’s a must for broadband connections. A software firewall runs on your PC and can protect you from both inbound and outbound attacks.
13. **Check your accounts and credit reports regularly.** Identity thieves can begin using your personal information to open accounts, purchase goods, and make your life miserable within minutes of obtaining that data. Check your bank account and credit card statements frequently. That way, if you discover that your personal information has been compromised, you can alert credit companies and banks immediately, so they can close your accounts.

Source:

http://www.mcafee.com/us/threat_center/tips.html