

Ten Tips To Secure Your Personal Computer



Securing your personal computer plays a crucial role in protecting our nation's Internet infrastructure. Here are ten things you can do to keep your computer safe from hackers and viruses.

1. **Use "anti-virus software" and keep it up-to-date.** Anti-virus software is designed to protect your computer against known viruses. But with new viruses emerging daily, anti-virus programs need regular updates. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software.
2. **Don't open emails or attachments from unknown sources.** Be suspicious of any unexpected email attachments even if they appear to be from someone you know. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment.
3. **Protect your computer from Internet intruders—use "firewalls."** Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet.
4. **Regularly download security updates and "patches" for operating systems and other software.** Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Check your software vendors' web sites regularly for new security patches or use the automated patching features that some companies offer.
5. **Use hard-to-guess passwords.** Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long. Don't share your password, and don't use the same password in more than one place.
6. **Back up your computer data on disks or CDs regularly.** Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network.
7. **Don't share access to your computers with strangers.** Learn about file sharing risks. Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files." This ability to share files can be used to infect your computer or look at the files on your computer. Check your operating system and your other program help files to learn how to disable file sharing.
8. **Disconnect your computer from the Internet when not in use.** Disconnecting from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet.
9. **Check your security on a regular basis.** You should evaluate your computer security at least twice a year—do it when you change the clocks for daylight savings! Make sure you have the security level appropriate for you.
10. **Make sure your family members and/or your employees know what to do if your computer becomes infected.** People should know how to update virus protection software, how to download security patches from software vendors, and how to create a proper password.

These tips were adapted from the "Top Ten Cyber Security Tips" on the National Cyber Security Alliance website, www.staysafeonline.info. The National Security Alliance is a public-private partnership focused on promoting cyber security and safe behavior online.

Report hacking incidents to the FBI at www.ic3.gov.



NATIONAL CRIME
PREVENTION COUNCIL

National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncpc.org