



7 PRACTICES for Safer Computing

- 1. Protect your personal information.** *It's valuable.* To minimize your risk of identity theft, don't share your personal information unless you know how it will be used and protected. Don't reply to or click on links in any email asking for your personal information.
- 2. Know who you're dealing with.** When shopping online, look for a seller's physical address and a working telephone number. Before downloading free software, read the fine print—some downloads come with spyware.
- 3. Use anti-virus and anti-spyware software, as well as a firewall.** Update them all regularly; many update automatically. Look for anti-virus software that removes or quarantines viruses, and for anti-spyware software that can undo changes spyware makes to your system. Make sure your firewall is on and set up properly.
- 4. Be sure to set up your operating system and Web browser software properly, and update them regularly.** Select security settings high enough to reduce your risk of being hacked. Make sure to regularly update your system with the latest patches.
- 5. Protect your passwords.** Keep your passwords in a secure place, and don't share them on the Internet, over email, or on the phone.
- 6. Back up important files.** If you have important files stored on your computer, copy them onto a removable disc, and store it in a safe place.
- 7. Learn who to contact if something goes wrong online.** Visit OnGuardOnline.gov and click on "File a Complaint" to learn how to respond if problems occur when you're online.

To learn more, visit OnGuardOnline.gov

STOP • THINK • CLICK™