Safe Computing:
Tips for understanding the common threats

Understanding the ups and downs of the Internet and online transactions is one of the best ways to start practicing "safe computing." Armed with a good understanding of common threats and a few practical tips to help you and your information stay secure, you can click to your heart's content.

Tip #1: Safeguard personal information

Don't fall for e-mail scams asking for your Social Security Number, bank account number, passwords, or any other private, identifiable information. Any kind of personal information should be protected, but most commonly, identity theives are in search of:

- Name
- Address
- Date of birth
- Social Security number
- Driver's license number
- Mother's maiden name
- Account numbers
- Card expiration dates
- Internet passwords
- Personal identification numbers
- User IDs for online account access
- Security codes form the back of credit and debit cards

Tip #2: Use good passwords

Some computer systems can be accessed remotely by scammers who want to gather and misuse your personal login and password information. If you have a weak password, your information is vulnerable to dictionary attacks, rapid automated guessing of common passwords. This is of special concern on systems where you've set yourself to log in automatically and may be unaware of a totally blank administrative password.

Here are a few tips to keep in mind:

- **Never share your password.**
  Even someone you trust could misuse your information. Keep this information exclusively private.
- **Never write down your password.**
  If you lose the piece your paper your password is written on, it could end up in the hands of identity thieves.
- **Change your password frequently.**
  The longer that you have used your password, the more likely it is that someone else will manage to figure it out. just how frequently you should change your password depends on how frequently you use it and what you are protecting with it. For example, you may wish to change a password used to give access to financial information more frequently.
- **Never store a password in a program**.
  Many e-mail and Web programs will offer to store your password for you so that you don't need to type it in each time you want to access your account. But this convenience makes it easy for thieves to recover your password if they have or obtain access to your computer. It is also possible for some computer viruses to recover your password from such stores and e-mail them to random people or post them publicly on the Internet.

Tip #3: Be spyware savvy:

Spyware is software loaded on your computer without your consent, and often without your knowledge. The goal is to monitor or control your computer use – you might receive a large number of pop-up ads, be directed to Web sites you don't want to view or lose use of your computer's systems. It might take a long time to open or save files, or you may receive strange error messages. Sophisticated spyware programs may even record your keystrokes to steal your passwords or other sensitive personal information, leaving you vulnerable to ID theft or other fraud.

To lower your risk of spyware infection:

- **Set your browser security high enough to detect unauthorized downloads.** Update your operating system and Web browser software – many offer free software "patches" to close holes in the system that spyware might exploit.
- **Use anti-virus and anti-spyware software and a firewall, and update them frequently.** A firewall blocks unauthorized access to your computer and will alert you if spyware on your computer is sending information out. Anti-spyware software should be set to scan on a regular basis – at least once a week – and every time you start your computer.
- **Download free software only from sites you know and trust.** Free software is often bundled with unsolicited spyware. Custom toolbars, games or peer-to-peer sharing software are common offenders.
- **Don't click on links inside pop-up windows.** Always close pop-ups by clicking on the "X" icon in the title bar. Or better yet, install a reputable pop-up blocking software.
- **Don't click on links that claim to offer anti-spyware software.** Ironically, links that claim to offer anti-spyware software often actually provide spyware and trick you into downloading it yourself. Take the time to read the end-user license agreement before downloading any software. If the license agreement is too hard to find or understand, it may not be a safe download.

Resources

The Consumer Protection Division of the Indiana Attorney General's Office works to safeguard the rights of Indiana citizens every day. If you have questions or complaints regarding safe computing, or other appropriate consumer issues, contact the Attorney General's Consumer Protection Division using the web address and phone number listed below, or visit www.in.gov/attorneygeneral for more information.