

## Safety Tips for Teens and Kids

Chat rooms targeted for young audiences also attract predators looking for young victims. Remember, there is no reality on the internet. People can pretend to be anyone, and often their

intentions are not good.

- ◆ **Don't believe everything you read on the Internet**, especially from someone in a chat room. It's incredibly easy to lie online and predators who want your trust will tell you whatever they think you want to hear.
- ◆ **Predators looking to build a relationship will look for clues on what you like, who you are and where you live.** Don't give this information out freely, especially if it can be used to find you.
- ◆ **Choose a random user name or screen name** that doesn't relate to you, your age, school, location or interests.
- ◆ **Do not download files a stranger has sent you.** They may contain viruses or inappropriate materials.
- ◆ **Do not view the webcam of a stranger.**

- ◆ **Don't try to meet someone in person that you met online,** never meet them alone.



## Ten Tips for Safe Computing

- 1 Protect your personal information** (name, birth date, Social Security number, banking and checking account or PIN numbers). To minimize risk of identity theft, don't share this information unless you know how it will be used and protected.
- 2 Don't be fooled by official looking emails from your bank or credit card company.** You should not reply or click on emails asking for your personal information. If in doubt, use your account statement to call the company directly.
- 3 Know who you're dealing with.** When shopping online, look for the dealer's physical address and telephone number. Call to make sure the number works.
- 4 Don't download software unless you know and trust the source.** Suspicious sites may contain viruses and spyware.
- 5 Only provide financial information on secure web sites.** Secure sites have a small padlock icon in the lower corner of your browser and the web address starts with "https" rather than "http."
- 6 Understand any offers you take.** Read the fine print and ask the company for more information if needed. Make sure you know the total costs, delivery date and any cancellation or return policies. Print out the information so you have documentation.
- 7 Use anti-virus and anti-spyware software and a firewall.** Update them all regularly. Look for anti-virus software that removes or quarantines viruses. Research reputable anti-spyware software that can undo changes made to your system. Make sure your firewall is set up properly and enabled.
- 8 Be sure to set up your operating system and web browser software properly.** Select security settings high enough to reduce your risk of being hacked and make sure to regularly update your system with the latest security patches from the manufacturer's web site.
- 9 Protect your passwords.** Keep your passwords in a secure place, and don't share them over the Internet, email or the phone. The longer the password, the better.
- 10 Back up important computer files.** Copy them to a removable disc and store it in a safe place.



## Protect Your Computer

*Don't click on any links in emails from sources you don't recognize. Be careful opening any attachments you're not expecting, even if they appear to be from friends. These can contain viruses and spyware that harm your computer.*



## Message from Attorney General Stephen Six:



Dear Kansans,

The Internet provides us with easy access to an incredible amount of information, entertainment and services. We can conduct business, catch up with friends and purchase products around the

world, all from the comfort of our home.

Unfortunately, the convenience of the Internet also opens the door to scammers, hackers and identity thieves who want to take advantage of unsuspecting consumers online.

As part of our continuing effort to protect Kansans, this brochure will help you stay safe and aware while you're online. Special tips geared for young adults are also included.

I hope this information helps you protect yourself from dangers lurking on the Internet. By becoming aware of these issues, you can reduce your chances of falling victim online.

Sincerely,

A handwritten signature in black ink that reads "Stephen N. Six".

Stephen N. Six

## Email Scams

Don't believe everything you read in an email. Con artists have found that email is a fast and inexpensive way to trick people out of their money.

- ◆ Don't invest with a stranger over the Internet regardless of their plea.
- ◆ If you receive an email that asks for help getting money out of a foreign country, don't respond, don't give them any information and don't pay any money.
- ◆ Remember, if something sounds too good to be true, it probably is. With most scams, once your money is out of your hands, it's probably gone for good.
- ◆ If you receive an email seeking your personal financial information, forward the message — including all the email addressing information — to [spam@uce.gov](mailto:spam@uce.gov)
- ◆ The best advice is to delete email offers from unknown parties. If you have lost money in an email scam, contact the Consumer Protection Division at 1-800-432-2310.



Consumer Protection/Antitrust Division  
120 SW 10th Avenue, 2nd Floor  
Topeka, KS 66612-1597  
(785) 296-3751 or 1-800-432-2310  
[www.ksag.org](http://www.ksag.org)

# ONLINE SAFETY



- *Email Scams*
- *Safety Tips for Teens and Kids*
- *Protect Your Computer*
- *10 Tips for Safe Computing*

Provided by Kansas Attorney General  
**Stephen N. Six**