

HOW TO AVOID SPYWARE AND VIRUSES

- **Be suspicious of all e-mail attachments**

Whether an e-mail attachment comes from a friend, a co-worker or an unknown, put it under the spotlight before you download it. Who's sending this to me? What's the filename of the attachment? What type of file is this attachment? (hint: anything you don't recognize should be scrutinized extensively) Was I expecting this file? Does this file have anything to do with the body of the e-mail message, or are they completely unrelated?

- **Be extremely cautious of links in e-mails and IM messages**

Follow the same procedure as e-mail attachments. Where is this link going to take you? Does it have anything to do with the message that was sent to me? What's the address of the link? (hover over the link to see the real address).

- **Read all unexpected messages and dialog boxes**

Whenever your computer pops up a message and asks you to make a decision, read that message carefully. Don't just blindly click on whatever pops up. Also, be aware of pop-ups that look like legitimate error messages enticing you to click on them. If the message is from an "anti-virus" that's not the brand you're using, then it's a fake. Click on the X in the top right corner to close these types of messages (not OK or CANCEL) - this will safely close the malicious message.

- **Be wary of security warnings that ask you to download or buy software**

Websites occasionally will ask you to download software in order to use special features. You'll get a "Security Warning" asking if you trust the company that wants to install this software. Your trust is to be earned, not given. Do not install it unless you know that it's absolutely necessary.

- **Don't believe everything you see**

Some viruses present you with a fake scan of your computer. It claims that your computer is infected and tells you that you need to download or buy something. Do not believe it, even if it looks official. If you see this type of message, you are most likely already infected.

- **Think twice before installing software from unknown companies**

Make sure you're dealing with a reputable software company. You can feel secure that software from a CD stamped "Microsoft" or "Apple" isn't going to contain a virus, but we don't recommend running software downloaded from an unknown source.

- **Don't trust messages coming from social networking sites (Facebook, MySpace, or Twitter)**

Many viruses are distributed through social media sites. Messages from strangers and friends should be scrutinized the same way emails are. Be especially careful of messages that are not typical of what the sender usually sends you, their account may be hijacked.

- **Avoid using add-on toolbars in your web browser**

Don't install those "helpful" little toolbars that sit at the top of your browser. If you are offered a toolbar when installing a program (sometimes they sneak in when you're installing an unrelated program, so pay attention, don't just click Next, Next, Next...) refuse it even if it comes from reputable sources like Google and Yahoo!. At the very least, it will clutter up your browser. At most, you will be observed, recorded and infected.

- **Say NO to junkware**

Avoid installing the free gadgets like DownloadHelper, smiley's, cursors, wallpaper, or free screensavers. These gadgets often contain spyware, that's why they are "free".

- **Be careful of P2P file sharing networks**

Stay away from P2P networks like LimeWire or Kazaa. If you must use them, pay careful attention to what you are downloading. If a file is anything but an audio, video or image, you can be almost certain that it's a threat to your system. Sometimes even audio and video files contain viruses.

- **Use Mozilla Firefox or Chrome**

Insecure web browsers are gaping holes through which malicious code gains entry to your system. Mozilla FireFox and Google Chrome are excellent web browsers with an emphasis on security.

- **Use McAfee Site Advisor to warn you about bad links**

When searching online (using Google, Bing, or Yahoo) it's often hard to tell which links are safe to click on. By using McAfee Site Advisor you can be certain that the website you're about to visit is free of spyware and viruses. Site Advisor warns you about potentially risky sites by adding rating icons to your search results.

- **Use common sense, don't rely on your anti-virus to protect you**

Common sense is the enemy of digital threats. Just because you have an anti-virus doesn't mean you're protected. It's just like wearing a seat belt - it may help when you hit trouble on the road but it doesn't mean you can start driving carelessly. And it doesn't mean it's safe to pull up to a stranger offering free candy. Think about the consequences of each action you take. And even if you're a careful driver, you can still make mistakes - that's what anti-virus and seat belts are for.

Have a safe and productive time on the Internet! If you're interested in more tips like this please email us at info@teknika.com