IT@Intel Technology Tips

Intel Information Technology
February 2011

Intel IT creates and publishes articles for Intel employees to educate them on a variety of information technology subjects. Our goal is to help them improve productivity, take advantage of new IT services and raise awareness on other IT topics of interest. We've modified these articles from their original version for sharing with external audiences.

# Seven cyber sins: Online mistakes you can avoid

*You've set up Internet controls, and anti-virus and spam filters to protect your family. But is it enough?*

You think your family is protected when they go online. After all, you've installed virus protection software, a firewall, and spyware detectors on your home computer. You keep up with the latest operating system and browser updates. And you've set up Internet controls to filter the information family members (and others) can see. But is it enough?

Today's kids and teens spend lots of time texting with friends, communicating online through popular social media sites, checking e-mail, and chatting on blogs and in chat rooms. They know where to go online for music, movies, and TV shows. "Free stuff" to download beckons at the click of a button. But do they really understand the risks and how to be safe in cyberspace?

Take this opportunity to share with your family these tips on how to avoid seven "cyber sins" commonly committed by kids and teens.

## 1. What's so wrong with cyber-bullying? Nobody takes it seriously…

Bullying is no longer confined to the school hallway or playground. Technology now allows bullies to harass their victims 24 hours a day, seven days a week. Instant messaging, social network sites, e-mail, and chat rooms can be used to humiliate and torment. And they can often times do so anonymously.

Avoid this mistake: If you're being bullied online, don't keep it a secret. Tell a trusted adult, and keep telling them until action is

taken. If it is school-related, make sure school officials are made aware of the problem. Bullies thrive on attention. Don't open or respond to messages from someone who is bullying you—but don't erase the messages, either. They may be needed to take action. Finally, never agree to meet with the bully in person!

## 2. Exchanging pictures and personal information with people you have met online

Not everyone you meet online is who they appear to be. Sharing seemingly innocent personal information or pictures online can expose your family to cyber bullying and the more serious dangers posed by cyber-predators.

Avoid this mistake: Don't communicate with strangers online, even those who say they're your age or a friend of your friend—they may not be who they claim to be. You may know not to give out your name or address, or a photo of yourself, but you still may be sharing details about yourself that a cyber-predator could piece together to identify and find you.

## 3. Not trusting your instincts online

Think that nothing bad could happen in cyberspace? Not so: 42 percent of students have been bullied online and 13 percent say it happens regularly.

Avoid this mistake: Don't continue with a chat or phone conversation, or remain on a Web site if you get the feeling something is wrong. When things don't seem right, they probably aren't. Get off the site, end the chat, or turn off the cell phone.

## 4. Why pay for music and movies if you can "rip 'n burn" for free?

You wouldn't walk into a store and steal a toy or candy bar, right? And you wouldn't take a book from a bookstore without paying for it. So why would you download the latest hit movies from a torrent site or "rip and burn" music that you don't already own? Make no mistake about it: if you're downloading films or burning music for free, what you're doing may be illegal!

Avoid this mistake: Unless you're certain it's a free giveaway, don't download any album, song, or movie without paying for it. If you do, you're breaking the law and could end up facing a hefty fine. Make sure you purchase such entertainment from respectable Web sites.

## 5. Downloading free apps loaded with spyware and adware

Just because something is free doesn't mean you should take advantage of it. Hackers rely on you to download free software so they can sneak in malware to give them access to your computer and steal any vital information you may have stored on your hard drive.

Avoid this mistake: Don't blindly click and download. If you get pop-ups asking you to install something, ask yourself, "Did I request this?" Chances are you didn't. And don't assume that clicking "no" or "cancel" will get rid of the annoyance. The pop-up could be designed to look like a Windows system alert, in which case the "buttons" all result in the same thing: spyware and/or malware on your system. Always close pop-ups using the "X" in the corner. If you suspect that the pop-up is rigged to install even if you close it using the "X" in the corner, use your Task Manager to close the application.

## 6. Sending or opening e-greetings without thinking

We've all received e-mails saying someone has sent us an "e-card." Such e-greetings typically arrive in one of two ways. The first is with an attached PDF, ZIP, or Adobe Flash* file. It could even be a Microsoft Office* document. When you open the attachment,

you infect your system with malicious software. The second way is when you click on a link in the e-mail message. As you get to the linked Web page, you're presented with a generic graphic that says, "Click here to receive your card." When you do, guess what? You infect your system.

Avoid this mistake: As is the case with downloading free software, don't blindly click on a link or open an attachment. Never open an e-greeting from someone you don't know. Check the name and the e-mail address of the sender. Confirm with that person that they actually sent you a greeting by sending them a separate e-mail from the address in your address book. If the e-greeting is an attachment, we cannot stress enough how dangerous it is to open it. The opportunity for that attachment to evade current anti-virus detection is incredibly high and should be avoided at all costs.

## 7. Falling for hoaxes and urban legends

You don't believe everything you hear, so why believe everything you read? As with anything you do in life, always exercise common sense when online. Hoax e-mails are particularly popular on the Web. Some are used to gather e-mail addresses, while others can have more sinister intent—such as the collecting of personal information.

Avoid this mistake: Don't take everything at face value. If you receive something you believe to be a hoax, do not forward it or respond. Keep an eye out for urgent hooks designed to get your attention ("Make money fast!") or melodramatic subject lines ("Dying girl needs your help!"). Don't forward e-mails that ask you to send it on to people you know.

**For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it.**



Printed in USA Please Recycle 0211/JLG/PDF