



Security Awareness Weekly Tips

Week 1 -- Tips to avoid malware

1. Update your antivirus and other software regularly. Antivirus software and other security applications require frequent updates to work properly. Without updated virus definitions, they can't identify the newest forms of malware. Unfortunately there are always susceptible periods between the time a new worm or virus hits the Internet and the time the updated antivirus definition is available.
2. Think before you click... You don't always need to click the "OK," "I Agree" or "Cancel" options to close pop-up windows. Windows can also be closed by clicking the X in the upper right corner or by using the Alt+F4 key combination in Windows.
3. Before downloading software from the Internet, carefully read the fine print. Sometimes the End User License Agreement (EULA) will contain information about additional – and most likely unwanted -- software included in the download. It's also best to download software from the developer's site whenever possible. And if you're asked to sign up for something, make sure you read and understand the options you're presented with. Sometimes the "No" option actually means "Yes."
4. Email links aren't the only places malware and trojans can hide. Instant messages, social networking sites, blog sites and video sites can also contain malicious code.
5. Avoid questionable web sites. Sometimes your system can get malware downloaded to it just from you browsing the Internet. (It's called drive-by downloading.) Free software sites, song lyric sites, and porn sites are notorious for this type of behavior.

Week 2 -- Web 2.0 Safety Tips

1. When you receive instant messages with links, pictures, or attached files, even if they appear to be from people in your contact list, verify that the sender is who they say they are. If you can't verify who it came from, close the message or delete the attached files. If you don't know the sender, delete the message.
2. If you use an AutoResponse when you're away and can't receive an instant message, don't reveal too much about where you are or how long you'll be gone. If you instant message from home, you might not want everyone to know that you're "away on vacation" and no one will be at your house until the following week. The same is true for an AutoResponse to email messages.
3. If you post pictures of yourself online, make sure they don't reveal any personal information... i.e. your name, school name, where you work, where you hang out. If you post pictures of anyone else (friends, relatives, etc.), get their permission BEFORE you post. Remember that any picture you post online has the potential to come back and haunt you.
4. Blog sites are like public diaries. Before you post, always re-read and think about what you've written. There's always the possibility that what you post may be misinterpreted by others. You should never use a blog site to slander or attack others.

5. Webcams allow users to communicate in real-time using both text and video. This provides a great way to interact with others. Just remember not to get carried away and share (or show) too much while you're online. Remember the video can be saved and posted or played again, and again, and again, and again.

Week 3 -- Tips to safeguard your privacy and keep confidential information secure

1. Don't leave copies or store sensitive information on portable devices (i.e. laptops, pdas, thumb drives). Portable devices are easy to steal or misplace. If you must carry sensitive information with you, encrypt it.
2. Don't send sensitive data via email. Remember unencrypted email messages can be intercepted and read by a third party. Email can also mistakenly find its way to the wrong person or email address. If it's unencrypted, the unintended recipient will have full access to any sensitive or confidential information.
3. Don't leave unattended confidential or sensitive data on the copier, printer, or fax machine. You should retrieve the information as soon as it prints. When you no longer need it, shred it.
4. Store system backup tapes in a secure location (not in a desk drawer at work or in your car).
5. Make sure you properly erase data from old computer hard drives and portable storage devices. Just because a file has been deleted, doesn't necessarily mean that it can't be retrieved. Reformatting doesn't even ensure that data is gone. If you're going to get rid of an old hard drive or portable storage device, use one of the various software programs designed to sanitize drives completely. (Do a Google search for drive sanitizers.)

Week 4 -- Online safety tips for kids

1. If you use a public computer at school or in the library for instant messaging, don't select the "log on automatically" option. Someone using the computer after you might be able to log on with your credentials.
2. If an online experience makes you uncomfortable, don't be afraid to tell your parents or a responsible adult. The sooner you notify someone of inappropriate behavior, the more likely they'll be to catch the person and put a stop to it.
3. Be a good cyber citizen. Don't gossip, threaten or bully. You should show the same GOOD manners to people online that you show to those you communicate with in person.
4. Don't believe everything you're told online. Sometimes the people you meet online aren't who or what they claim to be. Just because they say they're 14, play football and go to a neighboring school, doesn't mean it's true. It might be the 37-year-old neighbor that's been watching you from across the street.
5. Only give your email address or IM screen name to people you know. Make sure you remember to tell them not to give it to anyone else without first asking for your permission. Then you'll have a better chance of identifying email and instant messages from people you don't know.