HOW TO RECOGNIZE AND AVOID MALICIOUS SOFTWARE

BROUGHT TO YOU BY

GEEK EASY COMPUTERS

420 N. Church Suite 1
Kalamazoo, MI 49007
http://geek-easy.com
info@geek-easy.com
269-548-TECH (8324)

How to avoid and recognize malicious software

The Internet is an amazing source of limitless knowledge. You can research the origins of the word cat or reconnect with your high-school sweetheart digitally. You can order groceries online without ever talking to a cashier or choosing between paper and plastic. Unfortunately the Internet has a darker, more nefarious side. There are people make a living writing and creating convincing advertisements, email, videos, and personal profiles with the intent of exploiting your inability to discern the genuine from the fake.

Social engineering (the act of ‘tricking’ someone into giving information that they would consider confidential or private) is rampant on the Internet. There is a new strain of rogue viruses spreading like wildfire that take advantage of people’s inherent ability to be over-trusting. These fake anti-virus programs will sneak onto your system bundled with legitimate software, triggered via a malicious advert on a familiar site or even directly sent to you and thousands of others disguised as a message from a friend, coworker, or family member.

Quite often these malicious programs target weaknesses and flaws in common programs like Adobe Flash, Microsoft Internet Explorer or Oracle’s Java. These companies regularly release patches and updates to fix security holes, but sometimes not until the particular weakness has been exploited for months or years. While we recommend keeping all of your software up to date; this is not enough to stop viruses anymore. Education and protection are your best defense against modern malicious programs.

Knowing what to avoid, what is safe to install, and when to call for help are some of your best weapons in the battle to keep your systems, data and identity safe and secure. When in doubt, look to your IT department, your favorite computer store, or even Google. Quite often a simple Google search of “[insert software name] virus” will turn up useful information. Our technicians are always happy to answer questions and help you find out if the message you’re seeing is legitimate or malicious.

That annoying pop-up telling you “Updates are ready to install” is typically associated with Windows updates. These are safe to install and highly recommended. Occasionally they can cause problems with third-party software or other customized settings and programs, but these are almost always easier to fix and troubleshoot than a viral infection that slipped through the cracks because those updates were ignored or avoided. On the same track, Adobe products such as Flash, Reader and Acrobat are crucial to keep up-to-date. Viruses and spyware can be embedded in what seem to be legitimate PDF documents like vendor brochures or compliance procedures as well as flash-based videos and advertisements like the ones on YouTube or Facebook.

These are examples of commonly targeted programs for new exploits, security flaws, and the most frequently updated. Browsers are another digital goldmine for ne'er-do-wells from all over the world, intent on gaining unauthorized access to your computer. Once they gain access in some way, they can steal passwords or other information needed to read and send email, view your online banking or log in to Facebook, LinkedIn, Yahoo or even World of Warcraft accounts. They can also use your computer to attacking other computer systems including those of people in your address book. The best way to prevent this unauthorized access is to keep Internet Explorer, Firefox, Google Chrome, Safari, Opera or any other web browser you use fully updated including any plug-ins or add-ons. Apple computers were once safe from viruses, malware, spyware and other malicious software for the most part. Unfortunately the more the grow in popularity and become more like PCs (you can now install Windows on most Macs), the more susceptible they are to threats. For instance, Apple QuickTime and iTunes are both very common downloads with regular updates that include new features in addition to bug-fixes and security patches. Both are found on PC and Mac environments, and both can be targeted by maliciously formed video and audio files. We highly encourage you to keep these up to date as well.

Viruses can and will infect your computers with or without user interaction in some cases. It could be a file on your USB flash drive, in your inbox or a viral machine on your network infecting other unpatched and unprotected machines along the way. While this rarely happens nowadays, it can be devastating in a business environment. Think of the damage a virus could do if it were to infect every PDF or word document on a network or corrupt your QuickBooks company file. The damage could be endless if a virus infected servers critical to network and employee functionality.

Now that you have an idea of the severity of the multi-billion-dollar industry of cybercrime, what can you do to protect yourself? Education is only half of the equation. Even with active protection, no computer, mobile device, network or server is 100% secure. While real-time antivirus software from respectable brands such as Symantec, Kaspersky, Sophos, Vipre, and Microsoft are the ‘muscle’ in your protection toolbox, additional anti-spyware software has become a necessity. Programs like MalwareBytes Anti-Malware, SUPERAntiSpyware or the less-effective SpyBot Search & Destroy and Lavasoft AdAware can all add an additional layer of security. Modern versions of Windows and Mac OS also have security functionality that can greatly increase your chances of avoiding or defeating infection if utilized properly. Components like Windows User Access Control and Mac OSX administrator authentication can keep software from running or installing without typing a password or allowing the prompt.

Developing an “Acceptable Use Policy” is good first step in limiting exposure to the dark side of the Internet. A document like this outlines what Internet use is allowed on company computers, and creates awareness and accountability if the policy is ignored. A recent major innovation in fighting the spread of known malicious software has been developed by companies like OpenDNS and Google. By using the system Web browsers use to find sites based on their URL and blocking those known to spread malicious software, they can prevent the risk to a client computer before its accessed the site and sometimes even before the Anti-Virus software developers have included that particular virus in their ‘definition files’ and updates. For more information, contact us or visit http://code.google.com/speed/public-dns/ and http://www.opendns.com/. Both have free or low-cost versions for home and business use, are fairly simple to implement and require no maintainance.

In today’s digital world, information and technology security needs to be less hands-off and more proactive. Multiple methods of prevention, education, and awareness need to be employed to get and stay protected. Above all, read and research anything you click on, know what programs you are installing, and if common sense says you shouldn’t search for free music\software downloads, Internet gambling or worse, then don’t. The computer and, more specifically, the Internet are powerful tools that let you to do more with your life, work, time, friends and family, but they can also be a source of financial and emotional stress if used without caution.

Quick Reference Guide

Do: Run a paid Anti-Virus software from a respectable software developer.
Do: Run active Anti-Spware/Anti-Malware protection software.
Do: Read prompts, dialog boxes, and pop-up windows. Avoid things you didn't request.
Do: Install updates for Adobe, Java, Anti-Virus, Office, Windows and Web browsers.
Do: Search the name of the software or pop-up before allowing or installing it.
Do: Call or email support if you're unsure and cannot tell if a program is safe.
Do: Schedule regular scans of your Anti-Virus and Anti-Spyware software.
Do: Read title bars and the name of pop-ups and prompts. If it has an Internet Explorer Icon and says "Your Computer Is Infected," it's probably malicious.

Don't: Click on links from unknown sources.
Don't: Install programs, toolbars or other unknown software without verifying safety and necessity.
Don't: Open email or attachments from unrecognized sources especially with blank or suspicious subject lines.
Don't: Open unsolicited or unrequested email from IRS, ADP, US GOV, or other government and financial institutions. These can be strikingly convincing, but are almost always fake. These organizations will contact you via phone or postal mail with important information.
Don't: Provide passwords in email. No legitimate company or email will ever request them, as email is inherently insecure because it is typically sent in plain text.
Don't: Disable or ignore warnings from your Anti-Virus software or Windows. If they are informing you of a problem, they require your attention to remain protected.
Don't: Click next without reading and checking or unchecking specific items on even trusted software installers. Example: Java updates and installers have the "Ask toolbar" installer checked by default. While not necessarily harmful, it's software that you did not ask for bundled without your knowledge, and it is suggested that you uncheck that portion of the installer before continuing.
Don't: Provide your address, credit card information, birthday, or social security number to an untrusted company or individual.
Don't: Accept candy(or files) from strangers.

And always **DO** call Geek Easy with any computer related questions or issues! We are always here to help you!

Geek Easy Computers
420 N. Church Suite 1
Downtown Kalamazoo just west of the Transportation Station, behind Metro PCS
269-548-TECH (8324)
http://geek-easy.com
info@geek-easy.com

Links:

http://news.cnet.com/8301-1009_3-10152246-83.html
Study: Cybercrime cost firms $1 trillion globally

http://www.techrepublic.com/blog/security/calculating-the-true-cost-of-cybercrime/4438 Calculating the True Cost of Cybercrime