Title: Recognize SPAM and Malicious Download Links

Task:

You've heard the advice: Don't download or run software you're unsure of. Here's a quick review of the warning signs to stop you from taking unnecessary risks. Copied from an infoworld.com article.

Most people's computers get exploited in only a handful of ways. Among the most popular methods is tricking people into downloading and running Trojans. Often, unsuspecting users get socially engineered into running a malicious file or app by following a link in email or visiting a website.

It can be tough to spot the fake stuff, so here's what you should watch for.

Instructions:

1. Emails with links to suspicious downloads

Yes, you can be sent legitimate info in emails, but 99 percent of it is either garbage or malicious. Due to antispam measures, most vendors now use methods other than email to advertise and spread their software. You know better. Don't fall for this.

2. Promos for antimalware software, disk cleaners, and optimizers

Find out what your antivirus program looks like when it's scanning for malware, so when you see the fake one, you'll know the difference. In general, real antivirus programs will not pop up when you visit a website -- then begin scanning your computer and claiming you're infected with dozens of viruses. Real antivirus software pops up and tells you it has blocked *one* malware program. The fake stuff usually also wants to scan your whole computer.

Malware writers also like to hide their rogue creations in fake disk compressors and optimizer programs. Don't install computer optimization programs. Most of them, including the real stuff, are junk.

3. Websites that ask you to install software

It's the rare website that asks you to install an app or a plugin to enjoy its content. Most often the site has either been created or modified by hackers to trick you into installing software. Want to stay uninfected? Don't install software from websites unless you're 100 percent sure the software is needed and is a legitimate product.

This includes Java, Adobe Acrobat, and Flash. Be especially suspicious if you know you've already installed what is ostensibly required -- and absolutely reject the install if the link doesn't point to the legitimate vendor's website. Legitimate vendors do not let

other websites install their software. (The exceptions are legitimate proxy sites such as Download.com.)

4. The program you downloaded doesn't do what it said it would

Let's say you've followed a request to download and run software so that you can view an “encrypted” file. But after doing so, you can’t read the purported (bait) document. Or you downloaded an app that was supposed to speed up your computer, but it doesn't work. Some Trojan horse programs follow through with the promised action, but most don’t.

5. Your computer is much slower after installation

If you install a program and your computer runs much slower, you should suspect malware is at work, especially if the promised action fails to materialize. Sure, if you install a huge hunk of software, you can expect your computer to drop the pace a bit. But if you install a small program and your computer crawls like molasses, something is up.

6. Your antimalware tools have been disabled

Here's a huge warning sign: Your antimalware tools or firewall no longer work. Unless you downloaded and installed another antimalware product or personal firewall, the ones you are currently running should still be active. But many malicious programs start by disabling your current protection.

7. Task Manager does not start

Along the same lines, if you try to start Task Manager and it doesn't load, you probably have malware to blame. I’ve also seen Task Manager pop up for a second, then disappear. It's the same situation.

8. You can't uninstall the program

A legitimate program is required to include an uninstall option, but malware programs don’t like to be uninstalled. If the newly downloaded program doesn’t uninstall, look out. If it includes an option to uninstall, but doesn’t carry out the action, look out. Yes, uninstall routines sometimes get hosed and fail -- but usually not right away.

9. A funky end-user license agreement

Most people don’t read the end-user license agreement (EULA) before they install a program. I do -- and I’ve seen malicious acts spelled out in English. I’ve seen one EULA that claimed after the program was installed, my computer and data was its property and it reserved the right to disable any action I took to uninstall the program. That EULA certainly wouldn’t hold up in court, but at least it warned me.

What should you do?

When in doubt, chicken out and don't install. Close the browser if you have to. If it's truly legitimate software that you need to access a website, go directly to the vendor's website to download. For example, if you absolutely need Adobe Acrobat, open a new browser window, surf to adobe.com, and install it from there.

What if it's too late?

Fire up your antivirus scanner to see if it detects any abnormal activity. Better yet, if you have a Windows computer, use Microsoft's free Process Explorer utility that runs all active executables against up to 57 antivirus engines