Safe Computing

In a Web 2.0 World

By

Ken “The Geek” Harthun

Safe Computing in a Web 2.0 World

by

Ken “The Geek” Harthun

About the Author

Ken "The Geek" Harthun has been playing with geeky stuff since 1959 when he disassembled his first wrist watch. Unfortunately, as a six-year old, he didn't have the proper tools and the watch was ruined. He had better luck a couple of years later when he managed to hook up an old phone he found in the trash as an extension in his chemistry lab.

In 1963, his father gave him a Digi-Comp I computer . Ken quickly mastered the binary programming and his life-long interest in computers was launched. He has been working with computer technology since 1973 and advocating sensible security practices since 1989 when one of his employees infected a company computer with the Stoned virus. He quickly isolated the infected diskette and implemented strict security policies to prevent future infections.

Ken is currently employed as a systems engineer at a computer consulting firm, specializing in network and desktop security for small and medium businesses. He is particularly interested in cryptography and he's helped many a user develop safer computing practices.

Ken is a professional writer and blogger, contributor to Search Security.com, IT Knowledge Exchange, and produces Ask the Geek, his personal blog. He's a contributing editor for Dave's Computer Tips, Security Focus section. Ken is currently working on his first consumer-oriented book on computer security. You can follow him on Twitter, if such things interest you, and Ken always welcomes your questions and comments at askthegeek@kennyhart.com.

Safe Computing in a Web 2.0 World

by Ken Harthun

It isn't getting any better on The Wild, Wild Web, despite state and federal government attempts to arrest and prosecute those responsible for electronically-perpetrated criminal acts. Spyware and malware of all kinds are increasingly more stealthy and difficult to remove thanks to rootkit technology. With the advent of Web 2.0 and its emphasis on sharing and collaboration, web-based attacks are more prevalent than ever, especially those that rely on JavaScript and other scripting languages.

CAN-SPAM did little to deter or eliminate spammers, and today the spam problem is even worse thanks to huge botnets run by organized crime syndicates. Phishing attacks are harder to detect and more frequent. Recently, I spent the better part of two days cleaning up the aftermath of a mass mailer worm infection for one of our clients; their email is still being blocked by some servers. In its September 2005 issue, Consumer Reports said, "One Third Of Net Users Damaged By Malware." Considering that article is three years old, I'd wager that the number of infected computers has doubled since then.

In my job as a systems engineer for a computer consulting firm, I deal with the effects of malware nearly every day. My previous releases of this article listed the field-proven steps I recommend to everyone I know. It's been nearly three years since I last published these tips, but the steps haven't changed much; they just need to be brought up to date, and a new step involving disabling scripting in the browser has been added. Computer users still haven't learned safe surfing practices, however (will they ever?), and must modify their on-line behavior--particularly by applying the first step--for rest of these steps to be truly effective.

Did I mention these things are *proven*? They are. These are practices have been protecting computer users in homes and businesses for as long as I've been using them. This is free advice that's really worth something:

1. Repeat after me: I will NEVER, EVER click on any pop-up of any kind - NEVER, EVER. Not even on the "X" (it's usually safe, but why take the chance?). Use the key combination Alt-F4 instead; it safely closes the current window. In the slimy world of sleaze-ware, "No" means yes, "Cancel" means yes, "Close" means yes - ANY click on a button means yes. So many times users ask, "How did I get that? I clicked 'no' when it asked me!" Well, sorry, but you clicked, so they got you. NEVER, EVER CLICK!

2. Although Internet Explorer 7.0 has enhanced security and has been detached somewhat from the Windows operating system, it is still too big a target. Crackers are still writing malware that exploits IE security flaws. I recommend you use Firefox or Opera to browse the Web. (Some web sites still require IE, so you'll be forced to use it for those, but you should minimize its use otherwise.) Whatever browser you use, be sure you configure your preferences to block all unwanted pop-ups or install a pop-up killer like the Google Tool Bar. And while you're at it, re-read #1!

3. Patch your system. If you're still running XP, make sure you have at least service pack 2. If you're a home user, install service pack 3. (I still see systems that are running XP with service pack 1 or 1a, probably because they turned off automatic updates. While some argue against it, I recommend you turn them on.) And be sure to install any recommended security updates and patches for ALL software on your system, - especially Microsoft Office - not just Windows. If

you're running Windows Vista, you benefit from its enhanced security, but you still need to keep ALL of your applications patched. Secunia's Online Software Inspector is an excellent tool for scanning your system's applications to discover those that need updates.

4. Besides installing a NAT router (see *How to Secure Your Computer: Maxim #2*), run a properly-configured, proven software firewall. Don't rely only on Windows XP's built-in firewall - it blocks inbound attacks only (see this article) and it has flaws of its own (see this article). It will not stop back-door trojans, adware, spyware, and the like from "phoning home" with your sensitive information. (See this article for more info.) While Vista's firewall does offer outbound filtering, it isn't much better (see this article for more information). My favorites are the Comodo Personal Firewall (free), and the Sunbelt Kerio Personal Firewall (full-featured for 30 days, then runs free in limited-feature mode, $19.95/yr for full version).

5. Run a good anti-virus program. Choices abound. I have used AntiVir Personal Edition (free) and Grisoft's AVG (free). Other good ones are Avast! and Comodo AntiVirus.

6. Run multiple anti-spyware/anti-adware programs and keep them updated. I recommend: a. Spyware Blaster. This free program blocks adware and spyware from installing in the first place and is frequently updated; b. Ad-Aware. Scan weekly, more frequently if you are a heavy surfer; c. Spybot S&D. Run it on the same schedule as Ad-Aware; d. Microsoft's Windows Defender is an excellent product and is installed by default in Windows Vista. Configure it for real time protection and automatic updates. One of the best commercial anti-spyware applications is Sunbelt Software's CounterSpy. It is a PC World Best Buy award winner. Comodo BOClean:AntiMalware is also a good one and it's free.

7. Run a spam blocker to isolate junk e-mail. Most malware and all phishing attempts rely on spam. You want to isolate this stuff and delete it. NEVER, I repeat, NEVER, EVER click on a link in any e-mail you are not absolutely certain is legitimate. And to be as safe as possible, always type in the address of your bank, credit card companies, and any other site that you want to keep secure. (See #1 above and apply that principle to links, too!) One of the best programs is Open Field Software's ella for Spam Control. It uses wizards to "train" it to your personal specifications. There are free and paid versions that work with Outlook, Outlook Express. My clients swear by it. Another good program is Sunbelt Software's iHate Spam.

8. On Windows XP, set up a restricted user account and use that for routine tasks. Only log on with administrative privileges when you need to install or configure software. This will prevent rogue programs from affecting your system - they won't be able to install. You can activate the "run as" feature so you can do administrative tasks while logged in as a restricted user. Microsoft Knowledge Base article Q294676 explains how to activate and use this feature. If you are running Vista, you don't have to worry about this step: User Access Control (UAC) takes care of it.
9. Finally, disable scripting in your browser. If you use IE (you probably shouldn't, see Step 2), Tony Bradley gives you an excellent step-by-step procedure to accomplish this. Firefox users have a more elegant solution in the form of an add-on: NoScript. I use it on every PC. Scripts are blocked globally by default, but you can selectively activate them if you trust the site. For example, you can trust the main site's scripts but keep blocking any advertising or other third party scripts with no ill effects.

While total immunity is impossible - new infections and variations on existing exploits appear daily -

these nine steps will help prevent, catch, or clean 98 percent of the junkware out there. As for the other two percent - or if you are already badly infected - you'll need to hire a geek like me.

Ken Harthun is a systems engineer at a computer consulting firm, specializing in network and desktop security for small and medium businesses. He has been working with computers since 1973 and advocating sensible security practices since 1989 when one of his employees infected a company computer with the Stoned virus. He quickly isolated the infected diskette and implemented strict security policies to prevent future infections.

Ken is a contributor to Search Security.com, IT Knowledge Exchange, and Ask the Geek, his personal blog. He's currently working on his first consumer-oriented book on computer security. You can follow him on Twitter, if such things interest you. (If you use Twitter, this 5 Buck Twitter Trick might interest you.)Ken welcomes your questions and comments at askthegeek@kennyhart.com.