

Krebs on Security

In-depth security news and investigation



BLOG ADVERTISING

ABOUT THE AUTHOR



An important aspect of securing any system is the concept of “defense-in-depth,” or having multiple layers of security and not depending on any one approach or technology to block all attacks. Here are some links to tools and approaches that I have found useful in stopping malware from invading a PC. Your mileage may vary.

Learn, Memorize, Practice the 3 Rules



Follow Krebs’s 3 Basic Rules for online safety, and you will drastically reduce the chances of handing control over your computer to the bad guys. In short, 1) If you didn’t go looking for it, don’t install it; 2) If you installed, update it. 3) If you no longer need it, get rid of it! For more on these rules, check out [this blog post](#).

Keep Up-to-Date with Updates!

It shouldn’t be this way, but the truth is that most software needs regular updating. As a result, staying on top of the latest security updates can sometimes feel like a nagging chore. Not all software includes auto-update features that let you know about new patches, or if they do, many of these take their sweet time let you know. Fortunately, there are some tools that make it easier to learn when security updates are available. Secunia’s [Personal Software Inspector](#) is popular option. Another is File Hippo’s [Update Checker](#). Both are free.

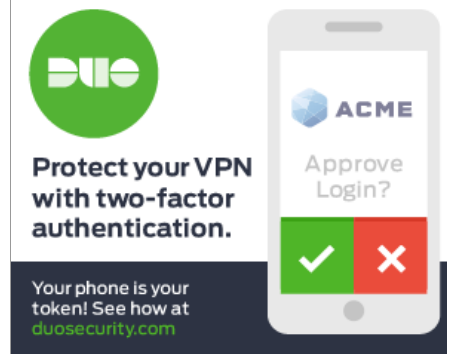
Put a Leash on Javascript

Most Web sites use **JavaScript**, a powerful scripting language that helps make sites interactive. Unfortunately, a huge percentage of Web-based attacks use JavaScript tricks to foist malicious software and exploits onto site visitors. To protect yourself, it is critically important to have an easy method of selecting which sites should be allowed to run JavaScript in the browser.

It is true that selectively allowing JavaScript on known, “safe” sites won’t block all malicious scripting attacks: Even legitimate sites sometimes end up running malicious code when scammers figure out ways to sneak tainted, bogus ads into the major online ad networks. But disallowing JavaScript by default and selectively enabling it for specific sites remains a much safer option than letting all sites run JavaScript unrestricted all the time.

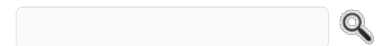
Firefox has many extensions and add-ons that make

Advertisement

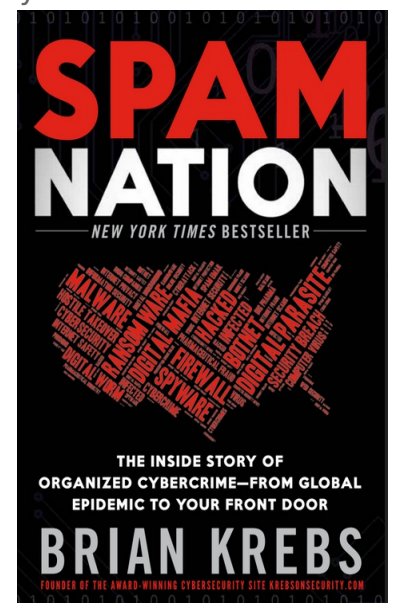


Protect your VPN with two-factor authentication.

Your phone is your token! See how at [duosecurity.com](#)



!KDM



A New York Times Bestseller!

Buy at Amazon 

stop tree

[Scientology Seeks Captive Converts Via Google Maps, Drug Rehab Centers](#)
[How to Spot Ingenico Self-Checkout Skimmers](#)
[Rise of Darknet Stokes Fear of](#)



surfing the Web a safer experience. One extension that I have found indispensable is **NoScript**. This extension lets the user decide which sites should be allowed to run JavaScript, including Flash Player content. Users can choose to allow specific exceptions either permanently or for a single browsing session.

Chrome also includes similar script- and Flash blocking functionality that seems designed to minimize some of these challenges by providing fewer options. If you tell Chrome to block JavaScript on all sites by default, when you browse to a site that uses JavaScript, the upper right corner of the browser displays a box with a red "X" through it. If you click that and select "Always allow JavaScript on [site name]" it will permanently enable JavaScript for that site, but it doesn't give you the option to block third-party JavaScript content on the site as NoScript does. In my testing, I had to manually refresh the page before Chrome allowed scripting on a site that I'd just whitelisted.

In addition, there is a very handy add-on for Chrome called **ScriptSafe** that works very much like NoScript. Please note that **Java** and Javascript are two very different things. Java is a widely-installed and quite powerful software package that requires frequent and attentive security patching. It plugs straight into the browser and is a favorite target for malware and miscreants alike. NoScripts and NoScript will both block Java applets from running by default. However, if you have Java installed, you're best off either **unplugging it from the browser**, or uninstalling it. Readers don't have to look very far on this blog for examples of why I recommend this, but **here's one**.

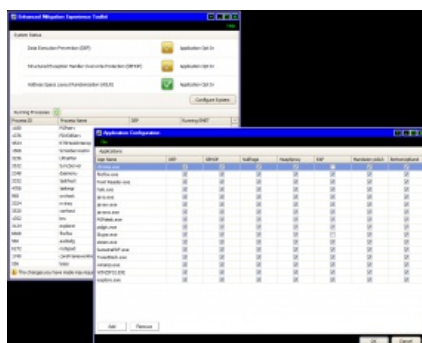
Internet Explorer allows users to block scripts, but even the latest version of IE still doesn't give the user much choice in handling JavaScript. In IE9, you can select among JavaScript on, off, or prompting you to load JavaScript. Turning JavaScript off isn't much of an option, but leaving it completely open is unsafe. Choosing the "Prompt" option does nothing but serve incessant pop-up prompts to allow or disallow scripts (see the video below). The lack of a simpler approach to script blocking in IE is one of the main reasons I continue to steer readers toward Firefox and Chrome.

Microsoft EMET

EMET, short for the **Enhanced Mitigation Experience Toolkit**, is a free tool from Microsoft that can help Windows users beef up the security of commonly used applications, whether they are made by a third-party vendor or by Microsoft. EMET allows users to force applications to use one or both of **two key security defenses** built into **Windows Vista** and **Windows 7** — Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP).

Put very simply, DEP is designed to make it harder to exploit security vulnerabilities on Windows, and ASLR makes it more difficult for exploits and malware to find the specific places in a system's memory that they need to do their dirty work.

EMET can force individual applications to perform ASLR on



The application page of EMET.

The Insider
Citing Attack, GoToMyPC
Resets All Passwords
Adobe Update Plugs Flash
Player Zero-Day

Impress

Please use your primary mailbox address, not a forwarded address.

Your email:

Enter email address...

Subscribe

Unsubscribe

Skills to IA



Click image for my skimmer series.

Circle of Hell



Badguy uses for your PC

Tools for a Safer PC



Tools for a Safer PC

Slampt

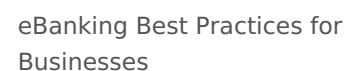
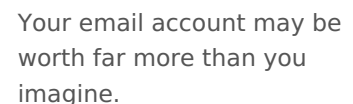
To proceed with EMET, **download the program** and install it. To wrap EMET's protection around a program — say, Internet Explorer — launch EMET and click the “Configure Apps” button in the bottom right corner of the application window. Selecting the “Add” button in the next box that brings up a program selection prompt; browse to C:\Program Files\Internet Explorer, and then add the “iexplore.exe” file. It should be okay to accept all of the defaults that EMET adds for you.

Prop up Your Passwords

If your email provider offers 2-step verification, take advantage of it. Gmail is one of the few that offers this added level of security, giving users a number of ways to receive the secondary logon codes. For more details on this service, read [this post](#). Facebook **also offers** a type of 2-step verification.

Also, don't forget to add a recovery email account, if your email provider supports it. And if possible, use two-step verification on that secondary account as well. **Here's a cautionary tale** about what can happen if you forget to add a recovery email address, or **forget to take full advantage** of 2-step verification.

Wireless and wired Internet routers are very popular consumer devices, but few users take the time to make sure these integral systems are locked down tightly. Don't make that same mistake. Take a few minutes to review these tips for hardening your hardware.



Online Cheating Site
AshleyMadison Hacked (798)
Sources: Target Investigating
Data Breach (620)
Cards Stolen in Target Breach
Flood Underground Markets
(445)
Reports: Liberty Reserve
Founder Arrested, Site
Shuttered (416)
Was the Ashley Madison
Database Leaked? (377)
True Goodbye: 'Using
TrueCrypt Is Not Secure' (363)
Who Hacked Ashley Madison?
(360)
Following the Money,
ePassporte Edition (353)
U.S. Government Seizes



For starters, make sure you change the default credentials on the router. This is the username and password that were factory installed by the router maker. The administrative page of most commercial routers can be accessed by typing 192.168.1.1, or 192.168.0.1 into a Web browser address bar. If neither of those work, try looking up the documentation at the

router maker's site, or checking to see if the address is listed [here](#). If you still can't find it, open the command prompt (Start > Run/or Search for "cmd") and then enter *ipconfig*. The address you need should be next to Default Gateway under your Local Area Connection.

If you don't know your router's default username and password, you can look it up [here](#). Leaving these as-is out-of-the-box is a very bad idea. Most modern routers will let you change both the default user name and password, so do both if you can. But it's most important to pick a **strong password**.

When you've changed the default password, you'll want to encrypt your connection if you're using a wireless router (one that broadcasts your modem's Internet connection so that it can be accessed via wireless devices, like tablets and smart phones). Onguardonline.gov has [published some video how-tos](#) on enabling wireless encryption on your router. **WPA2** is the strongest encryption technology available in most modern routers, followed by **WPA** and **WEP** (the latter is fairly trivial to crack with open source tools, so don't use it unless it's your only option).

But even users who have a strong router password and have protected their wireless Internet connection with a strong WPA2 passphrase may have the security of their routers undermined by security flaws built into these



routers. At issue is a technology called "Wi-Fi Protected Setup" (WPS) that ships with many routers marketed to consumers and small businesses. According to the [Wi-Fi Alliance](#), an industry group, WPS is "designed to ease the task of setting up and configuring security on wireless local area networks. WPS enables typical users who possess little understanding of traditional Wi-Fi configuration and security settings to automatically configure new wireless networks, add new devices and enable security."

But WPS also may expose routers to easy compromise. Read more about this vulnerability [here](#). If your router is among those listed as vulnerable, see if you can disable WPS from the router's administration page. If you're not sure whether it can be, or if you'd like to see whether your router maker has shipped an update to fix the WPS problem on their hardware, check [this spreadsheet](#). If your router maker doesn't offer a firmware fix, consider installing an open source alternative, such as **DD-WRT** (my favorite) or **Tomato**.

[LibertyReserve.com](#) (315)
[Extortionists Target Ashley Madison Users](#) (310)



Innovations from the Underground



ID Protection Services Examined



The reasons for its decline

OpenDNS

While you're monkeying around with your router setting, consider changing the router's default DNS servers to those maintained by OpenDNS. The company's free service filters out malicious Web page requests at the domain

name system (DNS) level. DNS is responsible for translating human-friendly Web site names like "example.com" into numeric, machine-readable Internet addresses. Anytime you send an e-mail or browse a Web site, your machine is sending a DNS look-up request to your Internet service provider to help route the traffic.

Most Internet users use their ISP's DNS servers for this task, either explicitly because the information was entered when signing up for service, or by default because the user hasn't specified any external DNS servers. By creating a free account at OpenDNS.com, changing the DNS settings on your machine, and registering your Internet address with OpenDNS, the company will block your computer from communicating with known malware and phishing sites. OpenDNS also offers a fairly effective adult content filtering service that can be used to block porn sites on an entire household's network.

Antivirus Software

This is probably the most overstated tool in any security toolbox. For years, security experts have been pitching the same advice: Install antivirus and firewall software, keep up with patches. Some companies even market their products with bold (and I'd argue misleading) guarantees like "Total Protection!". Here's the reality: Antivirus software is good at detecting known threats, but not so great at flagging brand new malware samples. If you're depending on your antivirus software to save you from risky behaviors online (downloading software from P2P/torrent networks, e.g.) you're asking for trouble. Again, it is best to think of antivirus as another layer of security for a modern PC.

There are a ridiculous number of free and premium antivirus services, the latter differentiated primarily by the inclusion of additional features, tweakable components and often live user support. If you value these bells and whistles and are in the market for antivirus software, here are a few buying tips:

Shop around: Antivirus companies make most of their money on renewals, and so steeply discount their products for new customers. If you buy a box version of commercial antivirus software at a big box retailer, you are almost certainly going to pay twice as much as you should. Check out the deals at Amazon.com and you'll see plenty of options for 3-PC licenses for between \$20 and \$30.

Re-buy, don't re-new: Also, when it comes time to renewing your antivirus subscription, avoid paying full price for it through the annoying reminder pop-ups that show up on your computer screen; just go shopping online again for another deal and buy a new subscription.

If you're fine with free antivirus, there are plenty of options. Here are a few (choose one*):

Avast

AVG Free

Avira Free

Bitdefender Free

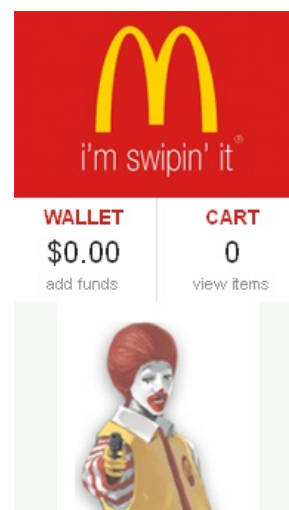
Comodo Free

Immunet (*Normally, it is not a good idea to have two different antivirus



File 'em Before the Bad Guys Can

psidca elis



A crash course in carding.

yt i r s la i c e s b

drf



Sign up, or Be Signed Up!

reldsc d r y s b

products installed at once, but Immundet was crafted specifically to work in tandem with other antivirus programs).

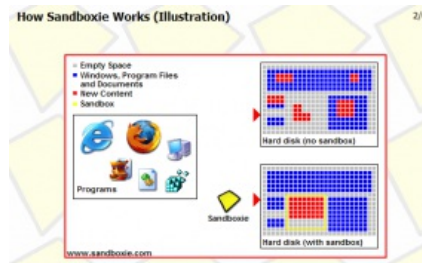
[Microsoft Security Essentials](#)

[Panda Cloud Antivirus](#)

[PC Tools Free](#)

[Force Apps to Play in the Sandbox](#)

If you're looking to add extra layers or protection, consider purchasing a license to [Sandboxie](#), which forces your programs to run in a protective sandbox that prevents said programs from making changes to the computer.



[Post-compromise](#)

Sometimes, even the best defenses fail. Falling victim to a Trojan, virus or worm attack is no fun, and cleaning up after such an infestation can be exceedingly difficult. Many experts believe that today's malware has become so tenacious that the only way to properly clean an infected machine is to completely wipe the computer's hard drive and reinstall a fresh copy of the operating system. I happen to count myself among this group, but I realize this is not a practical solution for many users. Depending on what type of infection your system has, it may be possible to remove the malicious software with the right combination of tools, assistance and determination.

First and foremost, seek help. There are several security help forums online that will happily assist users in diagnosing and fixing malware infections. Two of my favorite help sites include [DSL Reports' Security Forum](#) and [Bleepingcomputer.com](#). Please note that if you would like to tap the considerable expertise and knowledge of the help gurus at these forums, you will need to carefully read and observe each forums' rules on requesting help. These usually involve the requestor, wherever possible, to download, run and save the results of specific diagnostic tools *before* asking for help on the forums. Pay attention to the rules, be respectful and patient (the cleanup could take days), and you may be able to reclaim control over your PC at the end of the process.

[Combofix](#) is a malware removal tool that is extremely good at extracting difficult-to-banish malware and rootkits, malicious tools that attackers can use to burrow deep into an infected system. If a virus scan says you have some version of "TDSS" on your system, or you have an infection that comes back no matter what tools you use, try [TDSSkiller](#). Other handy removal tools include [Malwarebytes](#) and [Superantispyware](#). If you're trying to revive a computer that won't boot, check out my article with links to resources for [removing viruses from a PC that won't boot](#).

This tutorial was written as a list of how-tos and resources for the article, [The Scrap Value of a Hacked PC, Revisited](#).



Finding out is not so easy.

3



...For Online Safety.

