



## TECHNOLOGY INSIGHTS

These are our own opinions.

We have no commercial  
arrangements with vendors.

For more reviews, please  
contact TECHNOLEDGE.

T +61 2 9909 0246  
E [info@technoledge.com.au](mailto:info@technoledge.com.au)  
W [www.technoledge.com.au](http://www.technoledge.com.au)

## Driver Training

### A survival guide for the internet highway

#### PART 1 – STAYING OUT OF TROUBLE

##### Avoid temptation

The internet holds many dangers for the unwary. Temptations line the route, and traps await the traveller at every stop. Steering clear of trouble requires preparation and a steady hand at the wheel.

The starting point is to be wary of billboards that invite you to go to exotic places. There are many worthwhile destinations but those flashing signs that promise to shower you with prizes or wealth are suspect. If a pop-up tells you that there are issues on your PC that you can solve by downloading a free health check, get off the website as fast as you can. And if an email from your Bank asks you to confirm account numbers and passwords, call your Bank to verify the request. The phone is still a safe option.

The latest trick the malware merchants have devised is to hide their wares in images. The filters on most browsers and email clients are text-based and leave the door wide open to other kinds of attachments. An excellent article on how to avoid catching an email virus, including the kinds of attachments most likely to deliver it, is posted here:

<http://www.yourtechnonline.com/virus.php>

Email attachments are no longer the most common malware carriers. The bad guys have developed web pages that can inject spyware into PCs via browsers that don't have the latest security patches applied. This is called a 'drive-by download'.

Porn sites used to be among the most dangerous drive-by download sites, but they've been overtaken by peer-to-peer sites that offer free music downloads - Kazaa, Limewire, Morpheus and their ilk. Sites offering free videos and movies are best left alone unless they're known entities like Yahoo or your ISP.

Socialising sites like MySpace have also shot up the malware hit parade. You might make new friends there but chances are you'll also meet plenty of thieves. Signing up for new accounts, engaging in IM chat and downloading files can expose your personal data to people who can't be trusted. Also high on the dangerous places list are celebrity sites offering nude pics of Britney Spears or Paris Hilton. These days, they're said to be more risky than porn sites. It goes without saying that e-commerce sites require extra care since you're providing credit card details. And remember that screen savers, wallpaper, smileys and free games remain old favourites for hiding malware.

##### Read the Road

How do you tell a dodgy site from a legit one? With the crooks getting smarter by the week, it's getting harder and harder. You need help here, like a miner needs a canary on his shoulder. **McAfee's Site Advisor** is a good start. Like a handy set of traffic lights, the plugin marks the sites you visit in green, yellow or red on your search engine's list, including the ads. If it doesn't know the site, the colour comes up gray.

McAfee's canary may tweet too often, but it's better to err on the side of caution. **Site Advisor** is free, simple to install, has a small footprint and little impact on search speed. It works with both **Internet Explorer** and **Firefox**. You can read more about it and/or download it here: <http://www.siteadvisor.com/>

There are several other products that check the sites you visit for integrity.

**Netcraft** offers a free toolbar at <http://toolbar.netcraft.com/>

**Linkscanner** is another option - <http://linkscanner.explabs.com/linkscanner/>

**Mozilla's Firefox** offers dozens of browser extensions, including some that help keep you safe online. **NoScript** allows JavaScript, Java and other executable content to run only from trusted domains of your choice and prevents cross-site scripting attacks. <https://addons.mozilla.org/en-US/firefox/addon/722>

Another **Firefox** extension, still in beta testing but apparently stable, is *Firekeeper*.

<http://firekeeper.mozdev.org/index.html>

These early warning systems help you avoid known trouble spots. They won't stop you, but ignoring them could prove to be costly.

## Use the right vehicle

Three quarters of malware attacks are aimed at the **web browsers** and **email clients** we use. The more popular the program, the more hits it will get. **Firefox** became a popular alternative to **Internet Explorer** for that reason alone, but now it's become a target as well. **Opera** <http://www.opera.com/> and **Maxthon** <http://www.maxthon.com/> are smaller targets in more ways than one: they're leaner and faster than the two big guys, yet offer similar functionality. (Briard tries to engage with all of these in **Bowser Brawls – PART TWO** in **The Ragged Edge**)

The big target principle applies to email clients as well. That's why more and more users choose **Mozilla's Thunderbird** in preference to **Outlook** or **Outlook Express** - <http://www.mozilla.com/en-US/thunderbird/> .

**Eudora** is a longstanding favourite of heavy-duty users. Qualcom no longer supports the paid version, but the free version has ended up in the **Mozilla** camp. **Eudora** runs on Macs as well as Windows - <http://www.eudora.com/>

The popular Linux email program **Evolution** is another choice since it's been ported to Windows XP - <http://shellter.sourceforge.net/evolution/>

The **Opera** web browser includes an email client, and the small footprint of the combo eases the load on older PCs with limited resources.

One thing you need to check before changing browsers is that your AV software supports the one you're planning to switch to. Most AVs support **Outlook** and **Thunderbird** but, after those two, support gets patchy.

Browsers are more vulnerable than email clients these days, so it pays to tighten up the rules you want them to follow rather than rely on their default security settings. The links below provide some guidance for doing that.

**Internet Explorer:** <http://surfthenetsafely.com/ieseczone8.htm>

**Firefox:** [http://www.tweakguides.com/Firefox\\_5.html](http://www.tweakguides.com/Firefox_5.html)

Windows remains a huge target, of course. The updates can be a pain but most of them are designed to plug security gaps, so it's important to install them as soon as they become available. Changing to Linux might be an option if you want to spend less time worrying about malware, but that's a much bigger job than changing your browser.

**PART 2 – [SPAMS AND SCAMS](#)**  
**PART 3 – [AFTER AN ACCIDENT](#)**