Staying Safe on the Internet

David Harley BA CISSP FBCS CITP

On the Information Superhighway, the traffic lights are always at amber.
Here are some suggestions for reducing the risk from collisions and carjacks.

Table of Contents

Introduction

The traffic lights are always at amber on the Internet, because there are always risks, so here are some tips for reducing your exposure to attacks from cybercriminals. Of course, I can't cover all bases in a short document for every kind of cybercrime, not to mention the more traditional crimes committed via computer systems and networks. So we plan on a series of supplementary documents on "Staying Safe on the Internet", each of which will cover just one risk area in more depth.

Avoiding Malware

Well, you'd expect ESET to start here.... Make sure that your security software is updated regularly and automatically, but don't assume it will protect you from everything, and don't rely purely on antivirus software: multiple threats need multilayered protection like a full-blown security suite. (We can suggest a good one!) Keeping programs patched and updated also reduces the risks from "zero-day" attacks. Be suspicious of program files and Web links from any unexpected source, and be aware that even Microsoft Office documents, PDFs, image files and so on can sometimes conceal unpleasant surprises. Watch out also for fake anti-malware packages that detect imaginary viruses and spyware and are intended purely to cheat you out of your money.

Anti-Social Networks

Compressed URLs that use services like tinyURL.com, bit.ly and tr.im are convenient in tweets and texts and even in email, but they're very commonly used to disguise malicious Web sites with links to malware or to fake login screens. Treat very short URLs with suspicion. While we like to think that our Web pages are pretty secure, we prefer to use services that allow us to force you to view a preview of the real target URL before opening it. You can set an option on TinyURL's page in your own browser that does the same thing. "Web 2.0" sites are often fun but subject to worm attacks like Koobface, spam, and denial of service attacks.

Be careful not to post sensitive personal data on social network sites like LinkedIn, Facebook and Myspace: while such sites are getting better at restricting access to your profile, some of them have a long way to go, and you'd be surprised at what damage the bad guys can do with information you wouldn't think of as important. Take a birthday from one site, your home address from another, and some clever guesswork, and your identity could be as good as gone.

Maintaining a Healthy System

Keep your system and applications updated: make use of Windows Update and similar mechanisms for automatic updating, where possible. And while there are plenty of malicious sites that use drive-by browser exploits, don't forget that a lot of current malware reaches its target via PDFs, Microsoft Office documents and so on. So you need to keep applications like Adobe Reader and Office up-to-date with patches, as well as system updates. Don't use an administrative account for day-to-day work and play: using a profile that doesn't have administrator privileges is likely to restrict the amount of damage an attacker or malware can do if it does get access to your system

Protecting Your Passwords

Change your passwords frequently: painful though most of us find this, it does limit the extent to which your systems are exposed if something does get through. Use different passwords for different accounts and resources, so that if one does leak, it doesn't mean that an attacker has access to everything you own and every service you access. Use strong passwords or passphrases — a combination of upper- and lower-case letters, numbers, and other characters. Don't use passphrases that are easily guessed, and don't make silly mistakes like writing down passwords where they can easily be found, like on a Post-it attached to an encrypted USB drive.

(Don't Be) Burned on a Wire

Create a specific user profile without administrator rights for surfing from public hotspots, and avoid connecting to Web sites that involve the transfer of sensitive information, such as online banking. If you must access Webmail, use HTTPS. Even your home wireless network might be open to interception of your data by "Man in the Middle" attacks. WEP encryption, as used on many Wi-Fi networks, is weak and easy to crack: later protocols (WPA and WPA2) are better, but you shouldn't assume that they'll protect you from all kinds of attacks: wireless networks are intrinsically less secure. Avoid file/folder sharing and weak passwords for network shares.

Backups Not Crackups

Don't just back up to another folder or partition or even a second disk: hard disks don't last forever, and what if your PC is stolen or you have a fire? You may not think of your data as valuable till you lose it altogether. Do what professional system administrators do and keep backups "off-site." If you have a laptop that you take around with you, keep backing up so that if it's stolen or damaged, you won't have lost all that information (though you should still change passwords straightaway). Use system passwords so that it's more difficult for a thief to access your systems, and encrypt backed-up sensitive data that other people might have access to.

Don't Be Phish-Phingered

Phishing is not restricted to banks: crooks can make money out of all sorts of unexpected areas, like online gaming. Your bank should know your name: distrust all messages that aren't personalized, and check that Web links are to authentic sites.

Please Adjust Your Mindset

While following these guidelines will reduce your risks, you have another secret weapon: your own common sense. It's not just the settings on your computer that can save you from the hacker's grasp, but your own ability to think twice and not take things at face value. The most common Internet attack is social engineering, where the victim is manipulated into taking risks because he is insufficiently cautious about believing everything he's told. "Trust but verify": even messages from a trusted friend can be deceptive. It's all too easy to spoof (impersonate) an email address or Web site.

Let's be careful out there!

ESET Resources

- ESET Threatblog (TinyURL with preview enabled):
  http://preview.tinyurl.com/esetblog
- ESET Threatblog notifications on Twitter:
  http://twitter.com/esetresearch
- ESET White Papers Page:
  http://www.eset.com/download/whitepapers.php

Other Resources

- "Securing Our eCity":
  http://www.securingourecity.org/