Stay safe online: 5 secrets every PC (and Mac) owner should know

By Ed Bott | July 7, 2011, 5:11pm PDT http://www.zdnet.com/blog/bott/stay-safe-online-5-secrets-every-pc-and-mac-owner-should-know/3542

In any given week, I get dozens of requests for help. The #1 question of 2011? It's no contest:

"How do I protect myself online?"
These days I'm getting that question in equal numbers from PC and Mac owners who are concerned about the best way to avoid being sucker-punched by social engineering attacks.

Many people think that security begins and ends with antivirus software. I disagree. Should you run antivirus software? As I've said before, if you don't know the answer to that question, then the answer is yes.

So let's stipulate that you're running a well-supported, up-to-date security program—whether you use a PC or a Mac. What else do you need to do? In this post, I share the five steps I teach to friends, family members, and clients who want to avoid malware, scareware, phishing sites, and other online scams.

If you've been paying attention to the current threat landscape, much of the advice in this post will be familiar, even obvious. A lot of it is just common sense, but some is unconventional wisdom. Yes, of course you should expect to be attacked if you download porn or pirated software. But just staying out of bad online neighborhoods isn't sufficient anymore.

These days, threats can come from unexpected places: Google (and Bing) search results, compromised websites, deceptive ads, seemingly innocent downloads. You don't have to be doing anything out of the ordinary to inadvertently stumble across one of these potential threats.

If I had to summarize my guidance in a single sound bite, it would go something like this: ***Pay attention to your surroundings, and don't be stupid.***
Let's break that down.

Step 1: Don't panic.

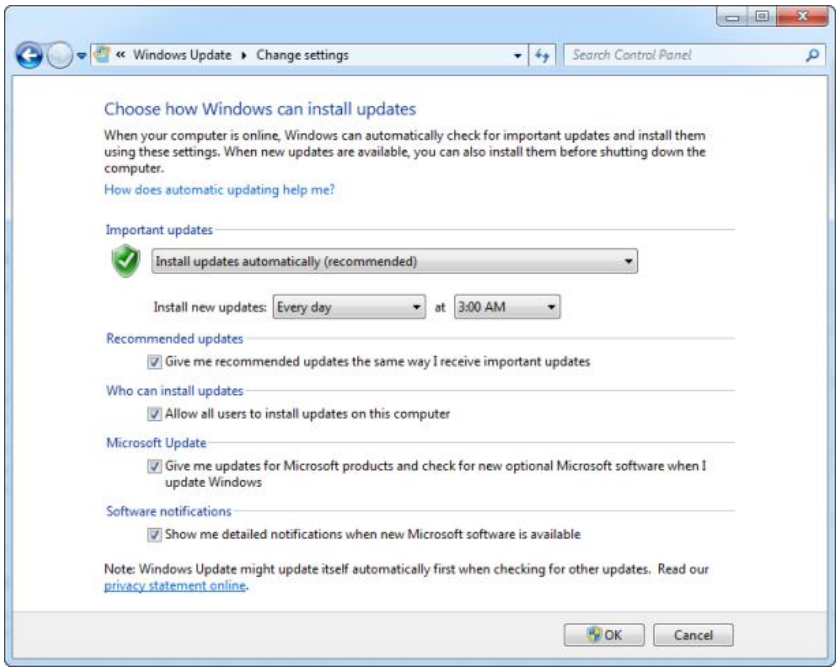
To borrow from a classic Monty Python sketch, the two … no, *three* chief weapons of online criminals are "fear and surprise…and ruthless efficiency." Their goal is to appear when you don't expect them and convince you to act hastily. Online criminals often play on fear *(your PC or Mac is infected with malware!)* or simple social engineering *(try these smileys! oh, and you need this codec—fake, of course—to play an enticing video clip).*
The antidote to Monty Python, of course, is Douglas Adams, for whom "Don't panic" was the secret of successful intergalactic hitchhiking.

When in doubt, stop. Think. Ask for help. If you're truly worried, pull the plug on your Internet connection temporarily until you can call a knowledgeable friend or drag the machine in to a specialist for a thorough diagnosis.
You should, of course, have a regular backup routine. Mechanical failures (a crashed hard drive or a dropped notebook) can be even more devastating than a malware attack. With Windows 7, you can use the built-in backup program to save an image backup on an external hard drive; you can do the same thing on a Mac using Time Machine. Restoring a full backup is easy, especially if the alternative is spending hours trying to track down a well-hidden infection.
And don't be paranoid. I can't count the number of times I've heard from otherwise smart people who break out all sorts of terrible tools—registry cleaners and system optimizers being the worst offenders—at the first sign of trouble. Those snake-oil programs, in my experience, tend to make the problem worse.

Step 2: Stay up to date.

Drive-by downloads and other sneak attacks are, fortunately, extremely rare. Yes, they happen, but the overwhelming majority of attacks aim at vulnerabilities that have been patched months or even years earlier.
Bad guys prey on the weak, technically unsophisticated, and ill-informed who don't update regularly. You really, *really* want to avoid being a part of that group. It's easy:

If you use Windows, turn on Windows Update and set it to automatically download and install updates. Those updates include Windows components like Internet Explorer. If you use other Microsoft software (Office, Silverlight, Windows Live Essentials, and so on) enable Microsoft Update, which is available from the Windows Update configuration screen.



If you use OS X, turn on Apple Software Update and set it to automatically download and install updates.

And don't overlook potential attacks from third-party software. ***On any platform, it is essential to regularly update not just the operating system and its components, but also any popular Internet-connected program.*** That means browsers like Chrome and Firefox, utilities like Adobe's Flash and Reader, runtime environments like Java and Silverlight and Adobe AIR, and media players like iTunes and QuickTime (on Macs, the latter two programs are included with system updates).

To make the process a little easier, I enthusiastically recommend Ninite, which automatically updates third-party software using the same URL you use to install the originals. It keeps unwanted add-ons and third-party programs at bay, too.

Since I wrote that post, Ninite has introduced a new product, the Ninite Updater, which "alerts you when any of the 92 Ninite-supported apps become out of date. It doesn't matter if your apps were installed with Ninite or not."
Alas, this utility is not free. The single-user package is $10 per year, and a 5-PC family pack is $30 a year. But it might be worth it for the peace of mind.

Home users can find a free alternative in Secunia Personal Software Inspector (PSI). Although it's nowhere near as comprehensive as Ninite's offering, it's a good way to cover the most important threats.

3. Learn how to make smart trust decisions.

As I mentioned at the beginning of this post, social engineering is the weapon of choice for online criminals these days. Attacks can take all sorts of forms, from conventional phishing e-mails to sophisticated and convincing malicious download sites. The best countermeasure? Education.

You're asked to make trust decisions many times every day. Some of those decisions involve programs, people, and businesses with whom you have lots of experience already. But others involve complete strangers, and still others ask you to decide with only limited information.

Any time you open an e-mail message or visit a web page, you face a possible trust decision.

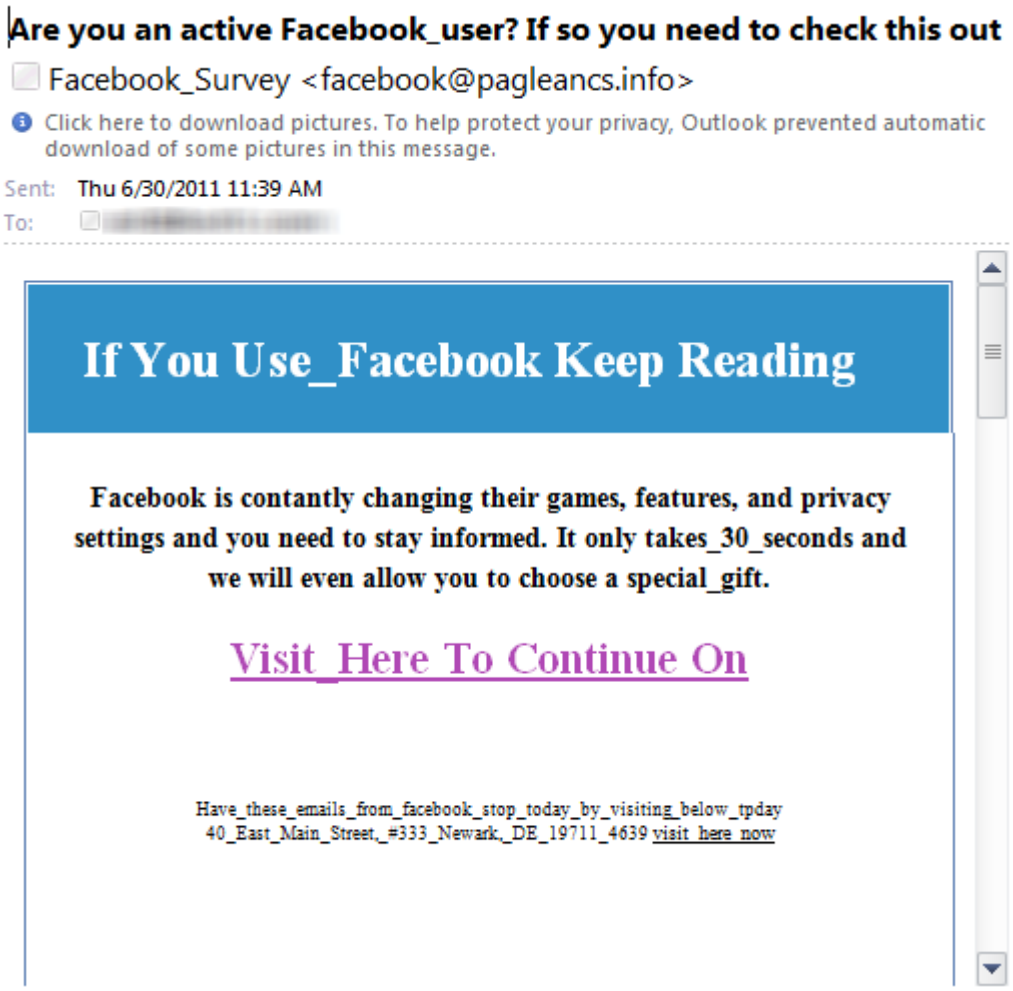
Should you trust the sender of an e-mail?
Spam is one of the primary vectors for phishing attacks and financial scams, but it's also a way to lure unsuspecting PC and Mac users to sites that deliver malware.

Spam filtering services have become very effective and can do a credible first pass on your inbox. The better your spam filter, the more likely it will recognize a fraud that could have sucked you in.

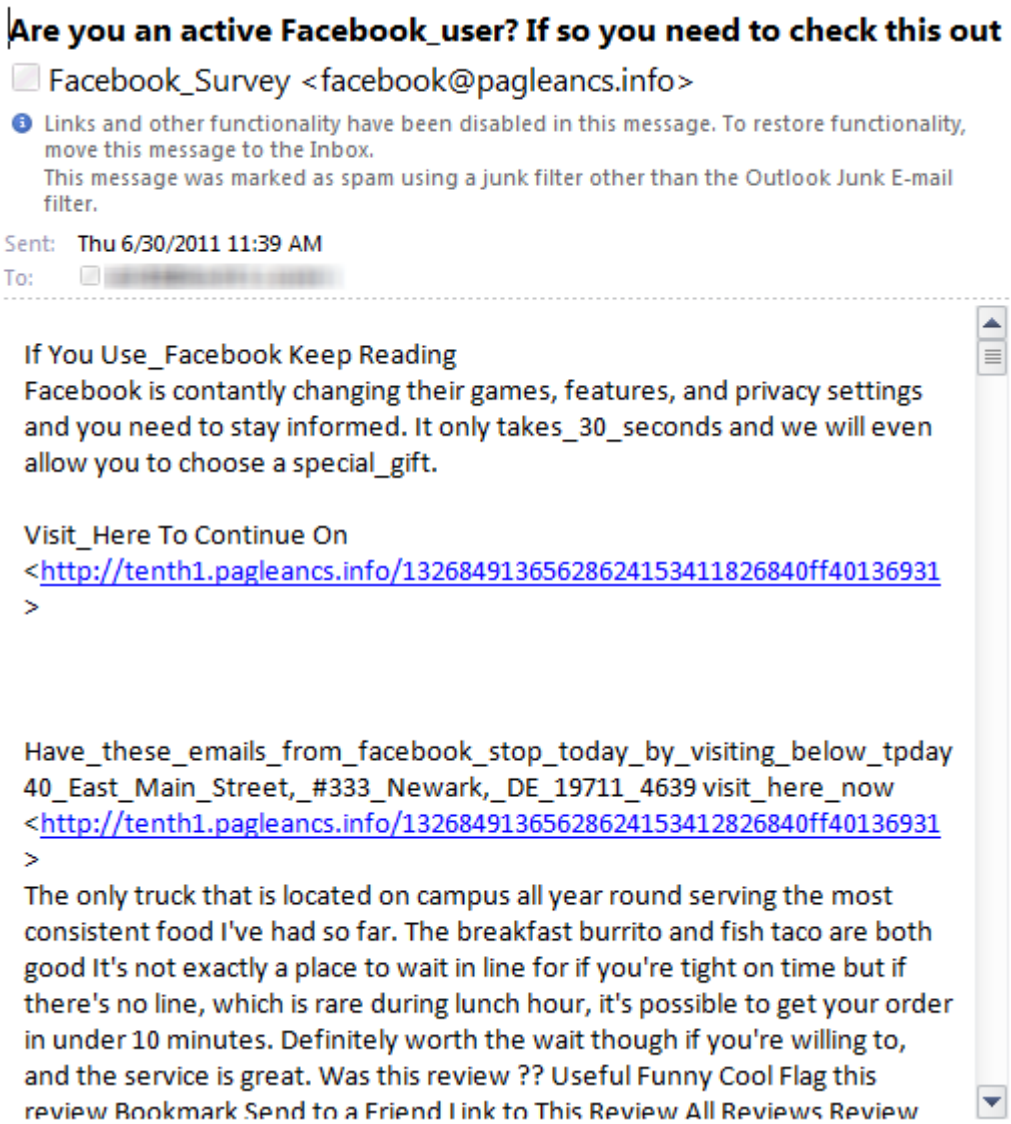
Based on my recent experience, both Hotmail and Gmail use extremely accurate spam-blocking technology. If your e-mail provider can't properly filter spam, consider forwarding your e-mail through a Hotmail or Gmail account.

And don't overlook the client program you use. Microsoft's flagship e-mail programs, Outlook and Windows Live Mail, display HTML-formatted messages differently when they are in the Junk folder.

Here's a crude but unremarkable phishing message as it appears in the Outlook Inbox folder. An unsophisticated recipient might be tempted to overlook the bad grammar and click.



But in Outlook's Junk E-Mail folder that same message is displayed in plain text, without graphics or HTML formatting. In addition, the hyperlinks show the actual target address in the message window. That turns the once-slightly-convincing message into a laughable mess, complete with bogus hidden text.



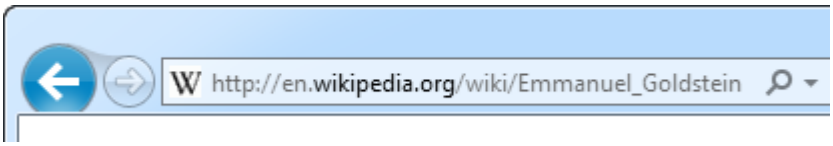
If the message appears to be from a friend or other known contact, it's possible that the sending account was hijacked. If you have even the slightest doubt about the actual target of a link, don't click it. That's doubly true if it's from a social network.

Should you trust a web page?

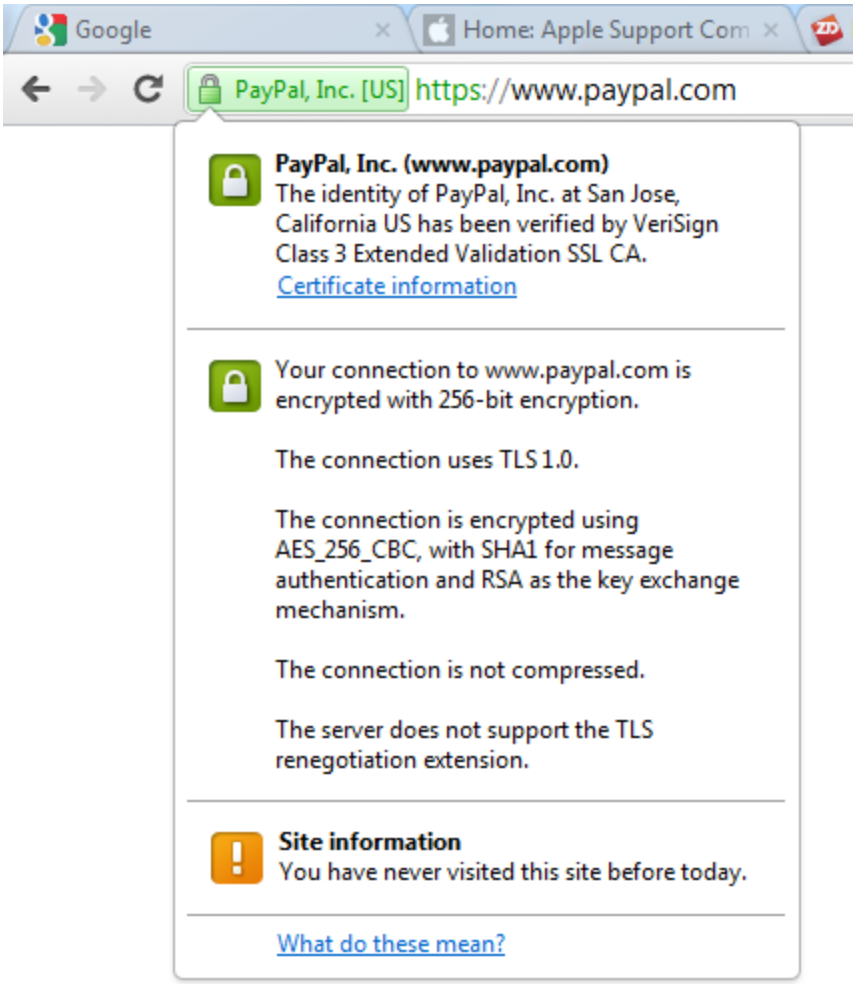
When using a browser, you need to learn how to read the address bar, especially at two key decision points.

First, anytime you are asked to enter your login credentials, your Spidey sense should tingle. You need to be able to spot a website that is trying to masquerade as someone else. If you have any doubt that a login page is legitimate, close the browser window and open a new session by manually typing the domain name and navigating to a login page from there.

Both Internet Explorer and Chrome provide important information in the address bar, displaying the actual domain name in black and muting the rest of the address to a still-readable shade of gray. Here's how it appears in Internet Explorer 9:



Second, learn how to identify a secure connection, where traffic is encrypted from end to end. Every modern browser displays visual cues (including a padlock icon) when you're using a secure SSL connection. For sites that use Extended Validation certificates, you get additional feedback in the form of a green address bar, as shown here for Chrome.



4. Never install any software unless you're certain it's safe.

The biggest trust decision of all arises when you're considering installing a new piece of software on a PC or a device. ***If you have any doubts about a software program, you should not install it. Period.***

One great way to remain safe online is to set a high bar for software. You need solid, up-to-date information to help you decide whether a file is safe, unsafe, or suspicious. Then you need information about whether the program is reliable and useful, whether it's compatible with other software you use, and whether it can be easily removed.

Here are the three key questions to ask about any program before clicking Yes on the installer:

Did it come from a trusted source?

It's hard to believe that someone would actually say yes to a software installer that randomly appears when they visit a web page. But people do, which is why fake antivirus software is a thriving business. The simple act of clicking No—or forcibly closing an installer window if necessary—can save you hours of cleanup.

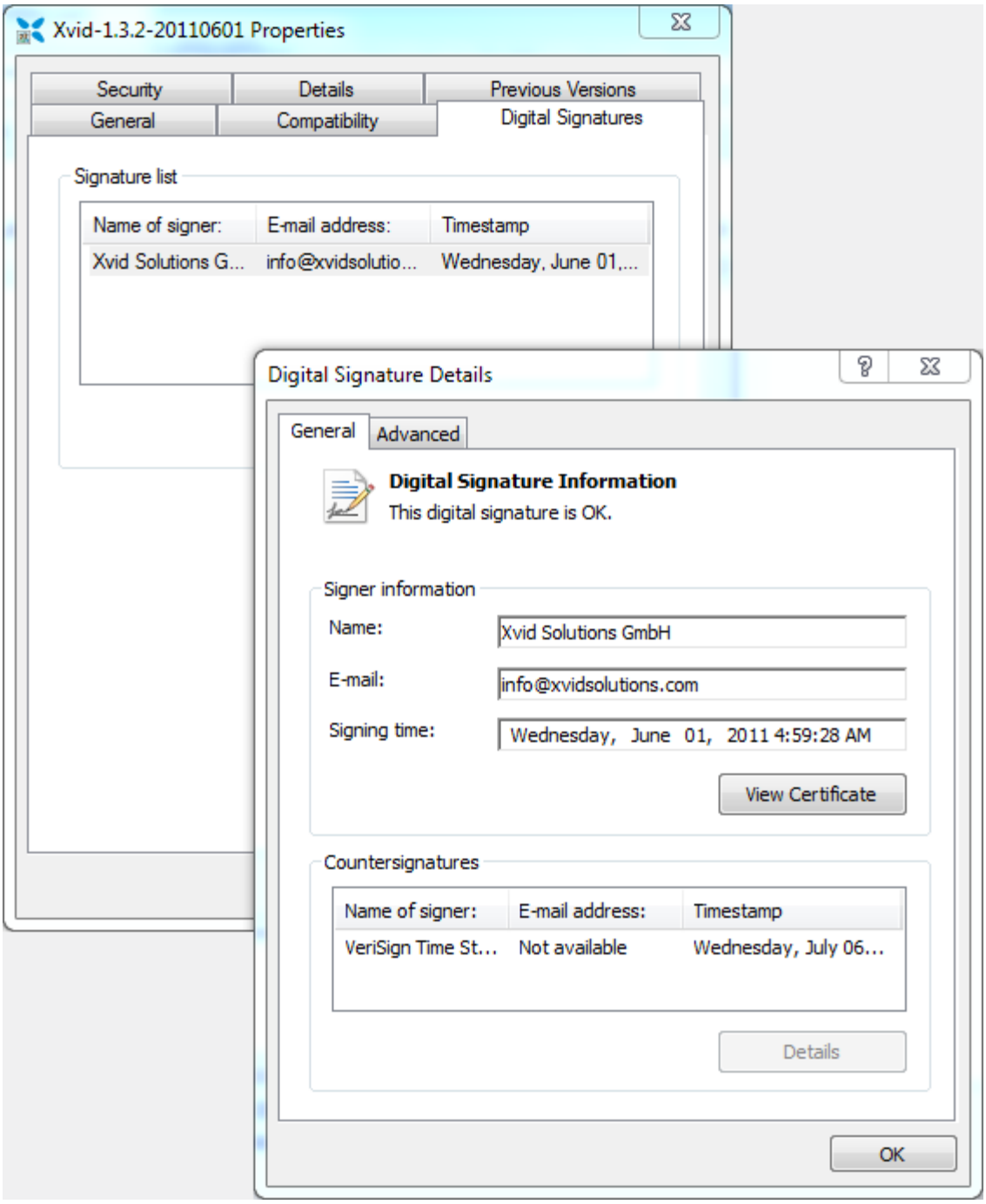
Is it signed with a valid digital signature?

In developing the SmartScreen technology used in Internet Explorer 9, Microsoft security researchers discovered a startling fact about the dangerous downloads they were blocking. I wrote about it earlier this year in IE9 versus Chrome: which one blocks malware better?

[T]he IE9 version of SmartScreen includes a new set of algorithms designed to test the reputation of this executable file. Has it been seen before? Is there anything about the file name or the domain that looks suspicious?

In fact, one of the most important questions to ask is this one: Is the executable file digitally signed? Microsoft's researchers found that roughly 96% of all those red warnings are attached to unsigned, previously unseen files. The algorithm assumes that a file—signed or unsigned—is untrustworthy until it establishes a reputation. No domain or file gets a free pass—not even a new signed release from Microsoft or Google. Every file has to build a reputation.

In Windows, you can check for the presence of a digital signature by right-clicking a file and choosing Properties. Here, for example, is the digital signature information for the officially released Xvid codec installer (the rogue version I describe in this post doesn't have a digital signature).

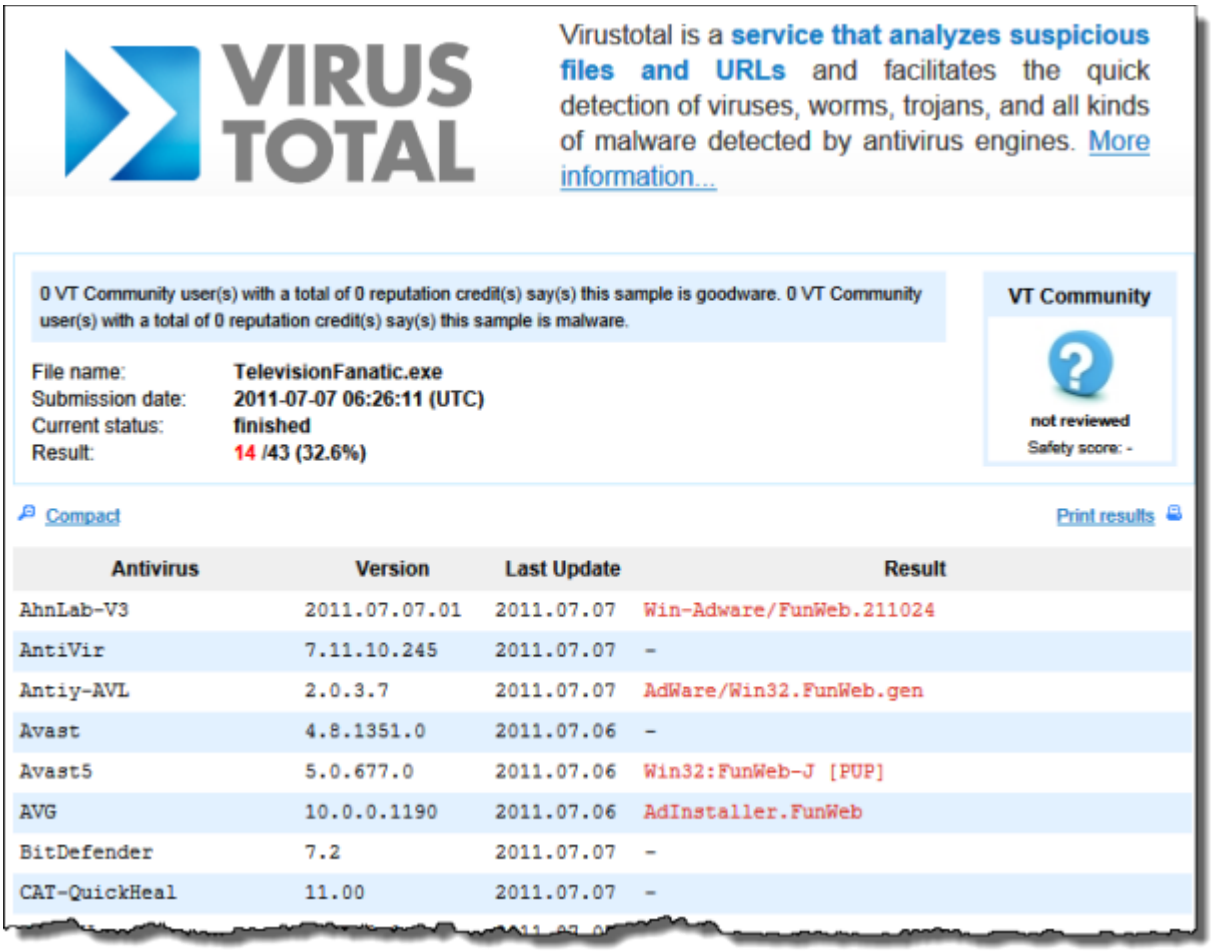


A digital signature doesn't mean a file is safe. It does, however, mean that you have important information, and a chain of trust, about the person or company who created the file. A digital signature also guarantees that the file hasn't been tampered with since it was signed.

In some cases, you might be willing to trust an unsigned file. You should only do so if you are confident that it is exactly what it claims to be and nothing more.

What does the security community say about the download?

If running a possible program through one antivirus scanner is good, then checking with 43 separate scanners must be, well, 43 times as effective. That's the theory behind Virustotal (VT), a free and independent web-based service. In a matter of minutes, you can upload a questionable file and have it checked by a large cross-section of scanning engines using up-to-date definitions. Here's what a Virustotal report looks like:



VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

VT Community

not reviewed

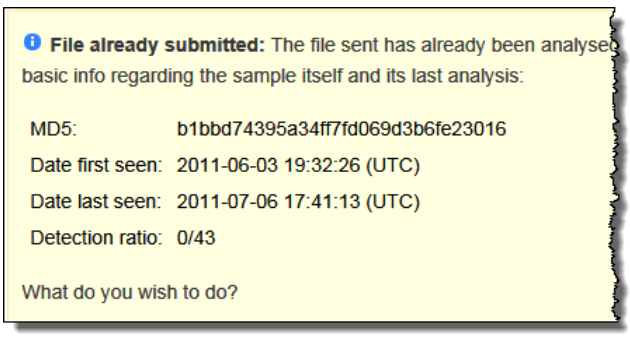
Safety score: -

File name: TelevisionFanatic.exe
Submission date: 2011-07-07 06:26:11 (UTC)
Current status: finished
Result: 14 /43 (32.6%)

Compact | Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.07.07.01	2011.07.07	Win-Adware/FunWeb.211024
AntiVir	7.11.10.245	2011.07.07	-
Antiy-AVL	2.0.3.7	2011.07.07	AdWare/Win32.FunWeb.gen
Avast	4.8.1351.0	2011.07.06	-
Avast5	5.0.677.0	2011.07.06	Win32:FunWeb-J [PUP]
AVG	10.0.0.1190	2011.07.06	AdInstaller.FunWeb
BitDefender	7.2	2011.07.07	-
CAT-QuickHeal	11.00	2011.07.07	-

One detail worth looking for when you submit a program is whether it's been analyzed by VT before. If the executable file you're analyzing is a well-known, established program, you can bet it's been examined already. Here, for example, is what I saw when I submitted a signed Xvid codec installer, obtained from a well-known and trusted site:



File already submitted: The file sent has already been analysed, basic info regarding the sample itself and its last analysis:

MD5: b1bbd74395a34ff7fd069d3b6fe23016
Date first seen: 2011-06-03 19:32:26 (UTC)
Date last seen: 2011-07-06 17:41:13 (UTC)
Detection ratio: 0/43

What do you wish to do?

If you're uncertain about a file, one option is to set it aside for 48 hours and then resubmit it to Virustotal. That's usually enough time for antivirus engines to identify a new strain of malware and add it to their definition files.

5. Be smart with passwords.

Has your favorite website been hacked lately? These days, it might be easier to make a list of the high-profile web sites that haven't been broken into.

Thanks to LulzSec and Anonymous, millions of people have had the dubious pleasure of seeing their usernames and passwords posted publicly on the Internet. Last month, LulzSec snagged more than 1 million accounts from Sony Music and Sony Pictures servers. The usernames, passwords, and personal details stored there were posted on the Internet for anyone to see.You might not be too concerned that someone can log on to your Sony account and pretend to be you. But what if someone goes to Google Mail or Hotmail and tries your email address and that same password? If you used the same password as the one on your Sony account, the bad guys are in. They can send and receive messages that appear to come from you. They can download your email archives, which can include correspondence from your bank and from online shopping sites like Amazon.com. In a very short period of time, they can do a very large amount of damage.

Repeat after me: Never use the same password in multiple places, and be especially vigilant with passwords for e-mail accounts.

It's a royal pain to create and remember unique, hard-to-guess passwords, but that is nothing compared to the misery you will experience if a determined thief starts messing with your identity and your finances.

Sadly, an awful lot of people reuse passwords, as software architect and Microsoft MVP Troy Hunt found when he grabbed those leaked Sony files, extracted 37,000+ pairs of usernames and passwords, and did some quick analysis. The entire analysis is a good read, but I zeroed in on this part:

When an entire database is compromised and all the passwords are just sitting there in plain text, the only thing saving customers of the service is their password uniqueness. Forget about rainbow tables and brute force – we'll come back to that – the one thing which stops the problem becoming any worse for them is that it's the only place those credentials appear. Of course we know that both from the findings above and many other online examples, password reuse is the norm rather than the exception.

Hunt compared the contents of the hacked Sony database with identical addresses from the Gawker breach of last year and found that two-thirds of the addresses on both lists used the same password. This ratio doesn't surprise me, and I suspect it might even be a little low.

If you're guilty of this offense, it might seem overwhelming to try to fix your entire collection of passwords at once. So start small, by creating new, unique, hard-to-guess passwords for your e-mail and bank accounts.

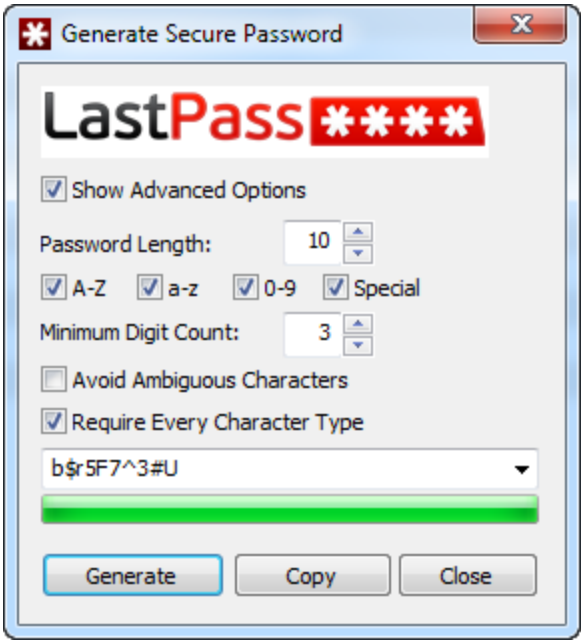
What makes a good password?

- It's at least 8 characters long, preferably 14 characters or more.
- It is not a word that can be found in any dictionary or list of common names.
- It uses at least three of the four available character types: capital letters, lower-case letters, numbers, and symbols (such as punctuation).
- It's easy for you to remember and difficult or impossible for someone else to guess.

And one more tip: if you anticipate that you will be entering a password regularly on a handheld device, consider how the virtual keyboard on that device works. Instead of a password like**Rh1ZJk#U**, consider grouping the different types of characters together for quicker input:**RZUUJ1hk#**.

The best way to create and manage strong, unique passwords is with the help of a utility tailor-made for that job. I recommend two:

LastPass is my favorite. It works on a wide variety of platforms and devices and lets you generate and save passwords that you can retrieve from anywhere. A security scare earlier this year led to LastPass tightening their security substantially, and they offer the option of two-factor authentication if you want extra security. The basic program is free, a premium version (worth it) is $10 a year.



If you’re queasy about the idea of having all your passwords stored on a web site, then consider RoboForm Pro. This program was one of my top 10 Windows programs a few years ago. Since then they’ve lowered the price dramatically, to $10 a year for unlimited devices. You can store your passwords in the cloud using the Online Sync service, or you can choose to store password data locally.