The 17 Most Dangerous Places on the Web

By Nick Mediati, PCWorld

Those photos of Jessica Alba may be murder on your PC. That Google search result that looks as if it answers all your questions may do nothing but create a serious tech headache. The fun you had watching that hilarious video you downloaded may not be worth the misery it can cause your system.

You've been warned that the Internet is something of a security minefield--that it's easy to get in trouble. You can do everything you can think of to protect yourself and still be taken by a malware infection, a phishing scam, or an invasion of online privacy. We'd like to provide a little help. Here are some of the hazards you may encounter, how dangerous they are, and what you can do to stay out of harm's way.

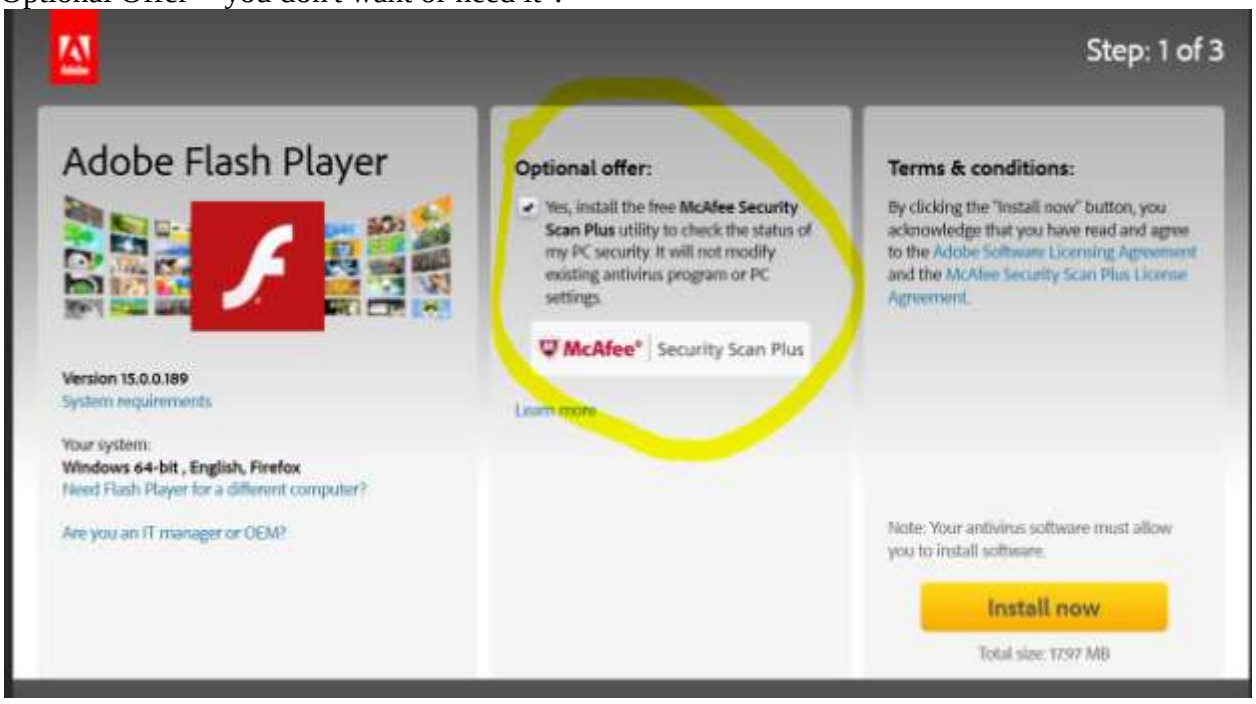
Not all Web dangers are created equal. Let our threat level indicator be your guide.

Threat 1 >> Malicious Flash files that can infect your PC

The Place: Websites that use Flash

Adobe's Flash graphics software has become a big malware target in recent years, forcing the company to push out frequent security patches. But another danger you might not know about is associated with Flash cookies. Flash cookies are small bits of data that their creators can use to save Flash-related settings, among other things. But like regular cookies, Flash cookies can track the sites you visit, too. Worse still, when you delete your browser's cookies, Flash cookies get left behind. (NOTE: You can configure the Flash plug-in to ask you before it downloads any Flash cookies.)

If You Have to Go There: To help protect against Flash-based attacks, make sure you keep your Flash browser plug-ins up-to-date. Never trust a "flash update" popup. Go to the source: https://get.adobe.com/flashplayer/ to download flash updates. (Be sure to UNCHECK the free Optional Offer - you don't want or need it".



Threat 2 >> Shortened links that lead you to potentially harmful places

The Place: Twitter

Scammers love Twitter since it relies so much on URL shorteners, services that take long Internet addresses and replace them with something briefer.

And it's very simple to hide malware or scams behind shortened URLs. A shortened link that supposedly points to the latest Internet trend-du-jour may be a Trojan horse in disguise.

If You Have to Go There: Simply don't click links. Of course, that takes some of the fun out of Twitter. The other option is to use a Twitter client app. TweetDeck and Tweetie for Mac have preview features that let you see the full URL before you go to the site in question.

Some link-shortening services, such as Bit.ly, attempt to filter out malicious links, but it seems to be a manual process, not an automatic one. TinyURL has a preview service you can turn on.

Threat 3 >> E-mail scams or attachments that get you to install malware or give up personal info

The Place: Your e-mail inbox

Although phishing and infected e-mail attachments are nothing new, the lures that cybercrooks use are constantly evolving, and in some cases they're becoming more difficult to distinguish from legitimate messages. My junk mailbox has a phishing e-mail that looks like a legitimate order confirmation from Amazon. The only hint that something's amiss is the sender's e-mail address.

If You Have to Go There: Don't trust anything in your inbox. Instead of clicking on links in a retailer's e-mail, go directly to the retailer's site.

Threat 4 >> Malware hiding in video, music, or software downloads

The Place: Torrent sites

Torrent sites (such as BitTorrent) are often used for sharing pirated music, videos, or software, and are a trove of malware. No one vets the download files--they may be malware in disguise.

Ben Edelman, privacy researcher and assistant professor at Harvard Business School, thinks torrent sites are the most dangerous places to visit, since they don't have a business model or reputation to defend (by comparison, many porn sites rely on being deemed trustworthy). "The [torrent] customers, they really don't want to pay," he says.

If You Have to Go There: It's probably best to avoid torrent sites entirely, given their untrustworthy content, but if you *must* visit, use a secondary PC to protect your main system. Use antivirus software, and keep it updated. Scan downloaded files and wait a couple of days before opening them. Brand-new malware can be tricky to catch, but the delay in opening may allow your antivirus software to get the necessary signatures.

Threat 5 >> Malware in photos or videos of scantily clad women

The Place: 'Legitimate' porn sites

Porn sites have a reputation of being less secure than mainstream sites, but that assumption doesn't tell the whole story. "There is no doubt that visiting Websites of ill-repute is deadly dangerous. If you make a habit of it, it's a given that you'll be attacked at some point," says Roger Thompson, chief research officer with security firm AVG. "Unfortunately, staying away from those sites won't keep you safe by itself, because innocent sites get hacked all the time, and are used as lures to draw victims to the attack servers."

And as mentioned earlier, many porn sites operate as actual, legitimate businesses that want to attract and retain customers. That said, it may be hard to tell the "legit" porn sites from malware-hosting sites that use porn as a lure.

If You Have to Go There: Be suspicious of video downloads, or sites that require you to install video codecs to view videos (see the next threat, below). Using tools like AVG's LinkScanner and McAfee's SiteAdvisor (or SiteAdvisor for Firefox) can help you weed out the malicious sites.

And, again, consider visiting such sites on a secondary machine. You don't want your browser history on the family PC.

Threat 6 >> Trojan horses disguised as video codecs, infecting your PC with malware

The Place: Video download sites, peer-to-peer networks

If you watch or download video online, you've likely been told to download a video codec--a small piece of software that provides support for a type of video file--at least once. Usually, these bits of software are perfectly legitimate, but some sites may direct you to download a piece of malware disguised as a codec.

If You Have to Go There: Your safest option is to stick with well-known video sites such as YouTube and Vimeo. And for catching up on the latest episodes of your favorite TV shows, sites and services like Hulu, TV.com, ABC.com, and iTunes are safer than peer-to-peer networks.

Threat 7 >> Geolocation--your smartphone and perhaps other parties know where you are

The Place: Your smartphone

The smartphone market is still in its infancy, really, and so are the threats. One possible concern is the use--or abuse--of geolocation. Although plenty of legitimate uses for location data exist, the potential for inappropriate uses also exists**. In one case, a game listed on the Android Market was in reality a client for a spy app**. Another site called pleaserobme.com showed a stream of FourSquare check-ins indicated that a person was away from their home (the site's goal, mind you, wasn't to condone theft, but to raise awareness of the issue). Apple recently updated its privacy policy to reflect changes in how it handles location data in iOS 4. The policy now states that "to provide location-based services on Apple products, Apple and our partners and licensees may collect, use and share precise location data."

If You Have to Go There: Be particular about the location-based sites, apps, and services that you use. On the other hand, weigh the privacy implications of services like FourSquare or the new Facebook Places feature, and consider how much you feel comfortable divulging. (Read more on how to retain privacy on FourSquare and Facebook Places.)

Threat 8 >> 'Poisoned' search engine results that go to malware-carrying Websites

The Place: Search engines

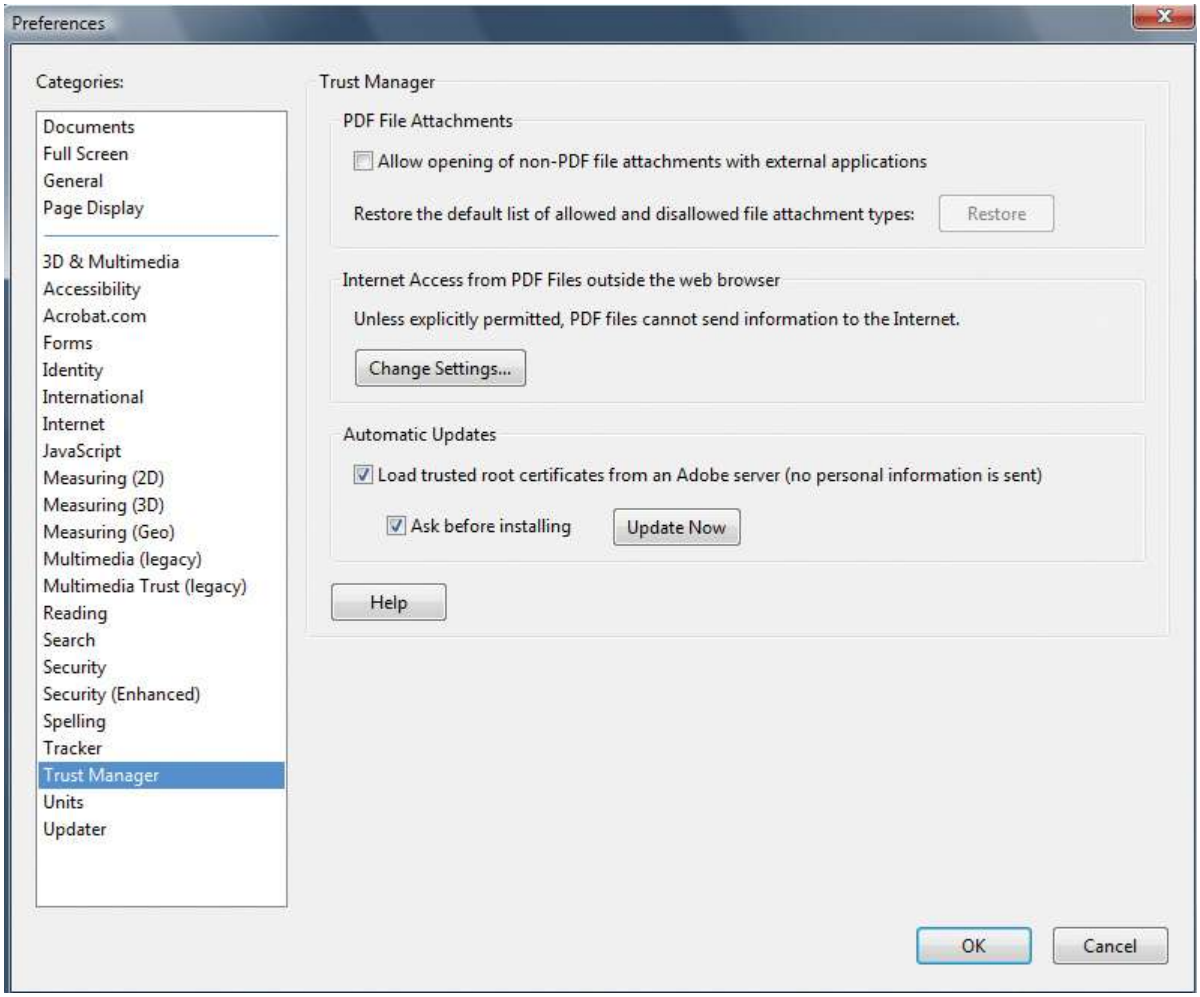
Search engine poisoning is the practice of building tainted sites or pages that are designed to rank high in a search on a given topic. For example, according to a recent study by the security firm McAfee, 19 percent of search results for "Cameron Diaz and screensavers" had some sort of malicious payload. Breaking news topics and Facebook are also common search targets for attackers.

If You Have to Go There: Pick and choose which sites to go to. Don't just blindly click search results; check each URL first to make sure that it really leads to the site you want. Although any site can be hacked, visiting the Washington Post's story on a hot news topic, for example, is probably a wiser choice than following a link to a site you've never heard of before.

Threat 9 >> Malicious PDFs that try to fool you into installing malware

The Place: Hacked Websites, plus your inbox

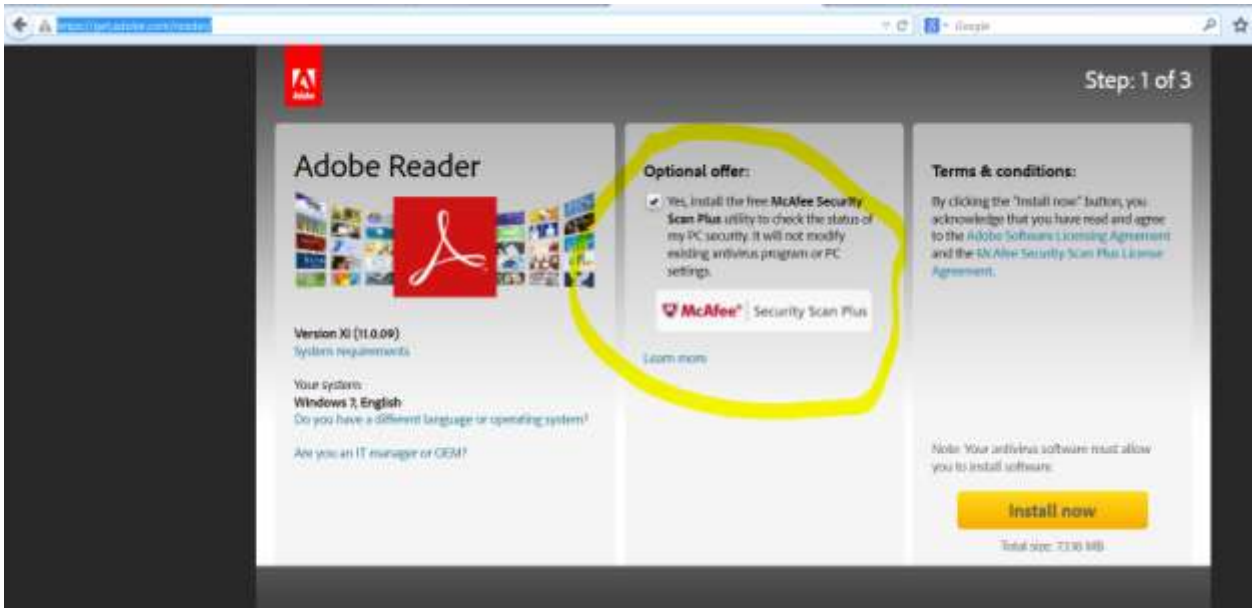
As Microsoft has become more serious about Windows security over the past few years, would-be attackers have had to find new ways to infect PCs. Attacking flaws in Adobe Acrobat is one of these newer methods. So-called poisoned PDFs are PDF files that have been crafted in such a manner that they trigger bugs in Adobe Reader and Adobe Acrobat; posted on a hijacked Website, they may let an attacker commandeer your PC and access your files and personal info. Feeling particularly paranoid? Uncheck 'Allow opening of non-PDF file attachments with external applications' (near the top) to head off certain PDF exploits.



A newer variant takes an otherwise innocent-looking PDF document and inserts malware into it. Adobe Reader may pop up an alert asking if you want to run the malware, but hackers can edit those messages to trick you into opening the file.

How serious is this problem? In 2009, attacks using malicious PDFs made up 49 percent of Web-based attacks, according to security firm Symantec.

If You Have to Go There: First, always make sure that you're running the latest version of Adobe Reader. Never trust a "Adobe Reader update" popup. Go to the source: https://get.adobe.com/reader/ to download Adobe Reader or the Updated Version. (Be sure to UNCHECK the free Optional Offer - you don't want or need it".



You can also use a different PDF reader, such as Foxit Reader. This can protect you from attacks on holes in Adobe Reader itself, but it won't make you immune to all PDF attacks, such as the newer ones that embed malware inside the PDFs. Make sure, also, that you update to Adobe to the most recent version of Adobe Reader by going directly to https://get.adobe.com. DO NOT trust the link to Adobe Reader Download found in a Google or Yahoo or MSN Search.

You can turn off Adobe Reader's ability to open non-PDF attachments by going to *Preferences*, clicking *Trust Manager*, and unchecking *Allow opening of non-PDF file attachments with external applications*.

Threat 10 >> Malicious video files using flaws in player software to hijack PCs

The Place: Video download sites

Attackers have been known to exploit flaws in video players such as QuickTime Player and use them to attack PCs. The threats are often "malformed" video files that, like malicious PDFs, trigger bugs in the player software that let the attackers in to spy on you, plant other malware, and more.

If You Have to Go There: Keep your player software up-to-date. Apple and Microsoft periodically release patches for QuickTime and Windows Media Player, respectively. Avoid downloading videos at random. Stick to well-known video sites such as YouTube, or to download services like iTunes.

Threat 11 >> Drive-by downloads that install malware when you visit a site

The Place: Hacked legitimate sites

A drive-by download occurs when a file downloads and/or installs to your PC without you realizing it. Such downloads can happen just about anywhere. Some sites are built to lure people into a drive-by download; but in a common attack method, criminals will hack a Web page, often on an otherwise legitimate site, and insert code that will download malware to your computer.

If You Have to Go There: The first thing to do is to keep your security software up-to-date, and to run regular malware scans. Many security suites can flag suspicious downloads.

Threat 12 >> Fake antivirus software that extorts money--and your credit card information

The Place: Your inbox, hacked legitimate sites

Fake antivirus programs look and act like the real thing, complete with alert messages. It isn't until you realize that these alerts are often riddled with typos that you know you're in trouble.

Most fake antivirus software is best described as extortionware or scareware: The trial version will nag you until you purchase the fake antivirus software-which usually does nothing to protect your PC. Once you send the criminals your credit card information, they can reuse it for other purposes, such as buying a high-priced item under your name.

You can get infected with a fake antivirus app in any number of ways. For example, in drive-by downloads (see the previous item), a malicious payload downloads and installs without the user realizing it or having any time to react.

If You Have to Go There: If you get an alert saying you're infected with malware, but it didn't come from the antivirus software you knowingly installed, stop what you're doing. Try booting into Safe Mode and running a scan using your legitimate antivirus software. However, such a scan may not clean up all of the malware-either the scanner doesn't have a signature for one fragment, or that piece doesn't act like traditional malware. The newer style of infections called Polymorphic Infections will slip past every current filter on the market. They morph (change) their file name and code script behavior each time they jump from one computer to another. This may render behavioral detection (which spots malware based on how it acts on your system) useless. **Quite often, you may need to call in a professional.**

Threat 13 >> Fraudulent ads on sites that lead you to scams or malware

The Place: Just about any ad-supported Website

Hey--ads aren't all bad! They help sites pay the bills. But cybercriminals have taken out ads on popular sites to lure in victims.

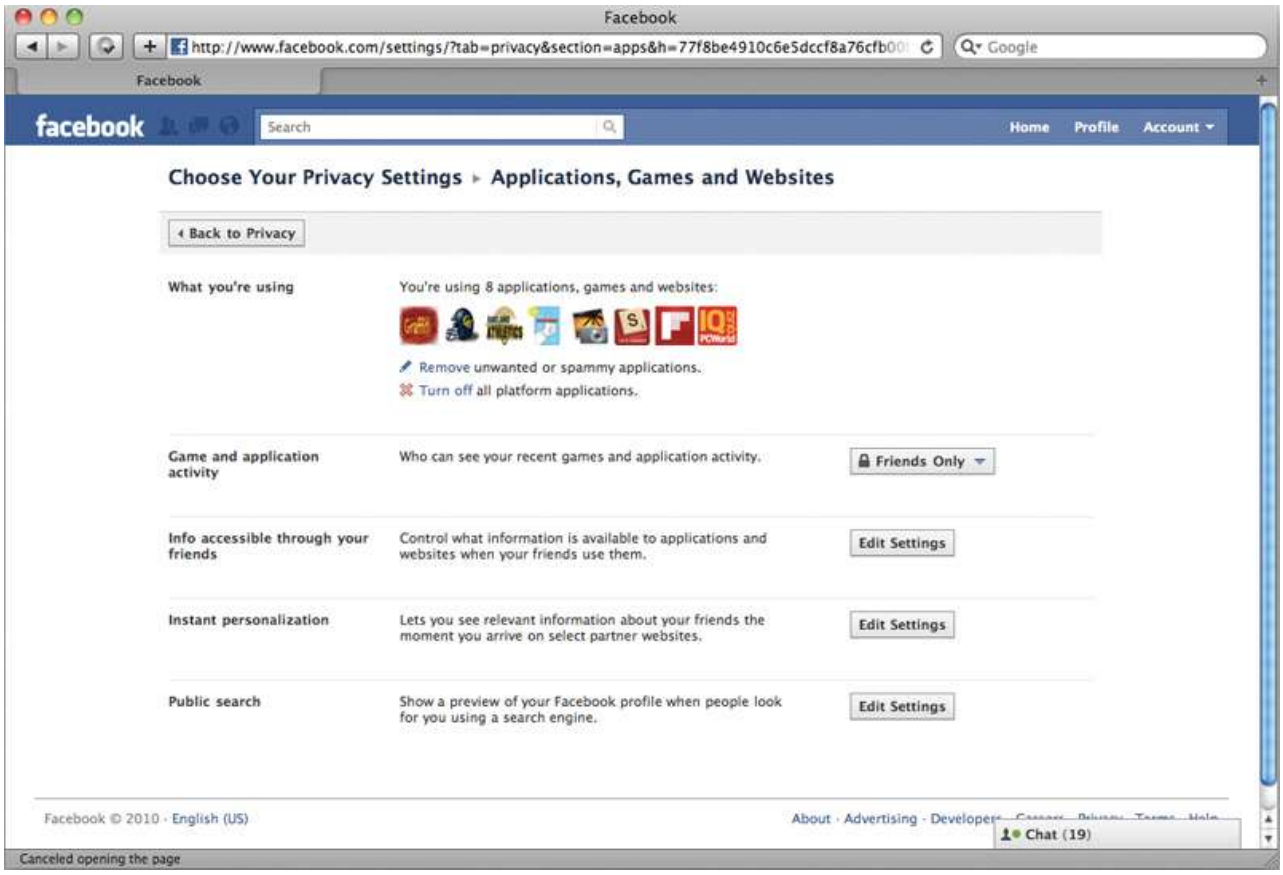
"The bad guys have become very clever at exploiting online advertising networks, tricking them into distributing ads that effectively load malicious content--especially nasty, scaremongering pop-ups for rogue antispyware," says Eric Howes, director of research services for security firm GFI Software. Google's Sponsored Ads and the New York Times online both recently ran ads on their pages that were frauds scamming to victimize the public. Neither Google or the New York Times were even aware until after the Ads ran.

If You Have to Go There: Most large sites have ad sales departments that work frequently with a core group of large advertisers, so it's probably safe to click a Microsoft ad on the New York Times site. But as the Google Sponsored Links incident shows, nothing is entirely fail-safe.

Threat 14 >> Questionable Facebook apps

The Place: Facebook

Facebook apps have long been an issue for security experts. You don't always know who's developing the apps, what they're doing with the data they may be collecting, or the developers' data security practices. **Take a few minutes to check your Facebook application settings to make sure that your app privacy settings are as you want them.**



If You Have to Go There: Be selective about the apps you add to your profile--don't take every quiz, for example. Check your privacy settings for Facebook apps, as well: Click the Account drop-down menu in the upper-right corner of Facebook's site, select *Privacy Settings*, and then click *Edit your settings* under 'Applications and Websites'. There, you can control which apps have access to your data, and which of your friends can see what information from apps (such as quiz results); you can also turn off Facebook apps altogether.

Threat 15 >> Sites that lure you in, get you to sign up, then sell your e-mail address for spam

The Place: 'Free electronics' sites

You've no doubt seen sites around the Web blaring, *Get a free iPad! A free iPod! It's easy!* These sites aren't typically dangerous -you probably won't get infected with malware-but your personal information could be sold to other businesses, who can then use it to sell more stuff to you.

If You Have to Go There: Read the privacy policies - CAREFULLY. Beware of privacy policy loopholes--even though a site says that it won't sell your private data to third parties, depending on the language of the policy, they may still be able to give your information to "affiliates."

Threat 16 >> Phishing 2.0 on social networks that tricks you into downloading malware or giving your Facebook login information to a criminal

The Place: Social networks

Questionable Facebook apps and malicious shortened links aren't the only dangers lurking on social networks. Sites like Facebook have given rise to new forms of phishing. Scammers might hijack one person's Facebook account, then use it to lure that person's friend into clicking a malicious link, going to spam sites, or giving up their Facebook login information--thereby giving scammers one more Facebook account to hijack.

"One of the bigger dangers currently facing users is malware, adware, and spyware spread through social networks like Facebook and Twitter," says Eric Howes, director of malware research with Sunbelt Software. "Users may receive spam via these networks offering them free deals, links to interesting videos, or even widgets to enhance their Facebook profiles. In many cases it is truly adware, spyware, or even malicious software that can exploit users' PCs."

If You Have to Go There: Don't trust every link posted to Facebook, even if one of your friends posted it. Be especially suspicious if the post is out of the ordinary for that person. Check the person's wall or Twitter @-replies to see if anyone is concerned that the person's account has been compromised.

And if you suspect that your account has been hijacked, change your password immediately. Both Facebook and Twitter have resources to help you keep up-to-date on the latest threats.

Threat 17 >> Oversharing--exposing too much personal information on your social network profiles

The Place: Social networks

How many times have you seen friends on Facebook or Twitter publicly divulge a bit more information than is necessary? Oversharing isn't just a matter of getting a little too personal--it can leave your private information viewable to the general public. But it's avoidable.

"There is a subtle danger that few people understand with the social networking sites, and that is the idea of information leakage," says AVG's Roger Thompson. "People, particularly teens, put all sorts of information online, without realizing that many more people than just their friends can see that data."

Oversharing could very well lead to more serious privacy issues further down the road, Thompson adds. "As today's young teens reach an age to apply for a credit card, I fully expect an onslaught of fraudulent card applications on their behalf, because they unwittingly divulged so much information. Harvesting is going on now, and we have no idea who is doing the harvesting."

If You Have to Go There: This particular threat is relatively easy to avoid, in that a little common sense can go a long way: Just be mindful of what you post. Do you really need to publish your home address and phone number to your Facebook profile?

Finally, be certain to check your privacy settings to make sure that you're not divulging your deepest, darkest secrets to all 500 million Facebook users.