How to Stop 11 Hidden Security Threats

Antivirus software and a firewall alone can't guarantee your safety. Here's how to foil the latest crop of sneaky attacks and nefarious attempts to steal your data.

Tony Bradley, PCWorld

Jan 24, 2010 9:00 pm

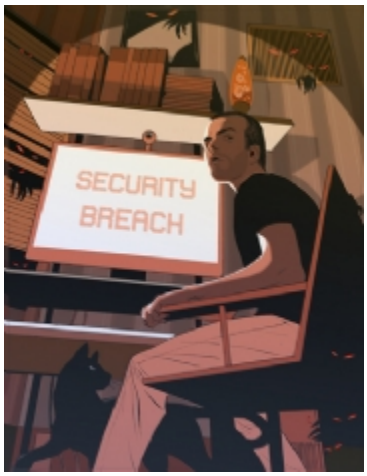


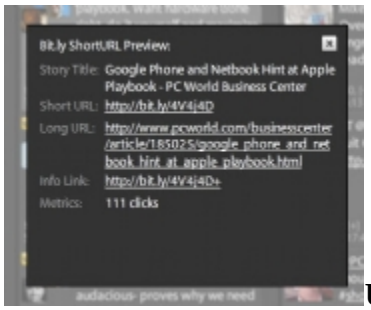
Illustration by Frank Stockton

Do you know how to guard against scareware? How about Trojan horse text messages? Or social network data harvesting? Malicious hackers are a resourceful bunch, and their methods continually evolve to target the ways we use our computers now. New attack techniques allow bad guys to stay one step ahead of security software and to get the better of even cautious and well-informed PC users.

Don't let that happen to you. Read on for descriptions of 11 of the most recent and most malignant security threats, as well as our complete advice on how to halt them in their tracks.

Shortened URLs

Most tweets, and lots of other electronic messages, include links that have been shortened by services such as Bit.ly, Tr.im, and Goo.gl. The URL aliases are handy, but they pose a risk, too: Since short URLs give no hint of the destination, attackers can exploit them to send you to malicious sites.



Use a Twitter client: Programs such as TweetDeck include options in their settings to display previews of shortened URLs. With such a setting enabled, clicking a shortened URL within a tweet brings up a screen that shows the destination page's title, as well as its full-length URL and a tally of how many other people have clicked that link. With this information at your disposal, you can make an informed decision about whether to click through and visit the actual site.

Install a URL-preview plug-in: Several Web browser plug-ins and services perform a similar preview function. When you create a shortened address with the TinyURL service, for instance, you can choose an option to create a preview version so that recipients can see where it goes before clicking. Conversely, if you're considering visiting a TinyURL link, you can enable its preview service to see the complete URL. For the TinyURL previews to work, though, you must have cookies enabled in your browser.

ExpandMyURL and LongURLPlease both provide Web browser plug-ins or applets that will verify the safety of the full URLs behind abbreviated links from all the major URL-shortening services. Rather than changing the shortened links to their full URLs, however, ExpandMyURL checks destination sites in the background and marks the short URLs green if they are safe.

Goo.gl, Google's URL-shortening service, provides security by automatically scanning the destination URL to detect and identify malicious Websites, and by warning users when the shortened URL might be a security concern. Unfortunately, Goo.gl has limited application because it works only through other Google products and services.

Data Harvesting of Your Profile

Some of the personal details that you might share on social networks, such as your high school, hometown, or birthday, are often the same items used in "secret" security questions for banks and Websites. An attacker who collects enough of this information may be able to access your most sensitive accounts.

Check your Facebook privacy settings: After signing in to your Facebook account, click *Settings* on the menu bar and select *Privacy Settings.*

Facebook's privacy settings allow you to choose who may see various personal details. You can hide your details from everyone but your Facebook friends (our recommendation), allow members of your networks to view your details as well, or open the floodgates and permit everyone to see your information. In addition, you can set the privacy level for each component of your profile--for example, your birthday, your religious and political views, the photos you post, and your status updates.

Don't accept any friend requests from strangers: From time to time you may get a friend request from someone you don't know. If you're serious about protecting your personal information, you shouldn't accept such requests.

Share with caution: Consider removing valuable information such as your birth date and hometown from your profile. You should also think twice before participating in Facebook quizzes and chain lists--though it seems innocent and fun to share your favorite breakfast cereal, the first concert you attended, or where you met your spouse, an attacker armed with enough of these tidbits can assume your identity.

Social Network Impostors

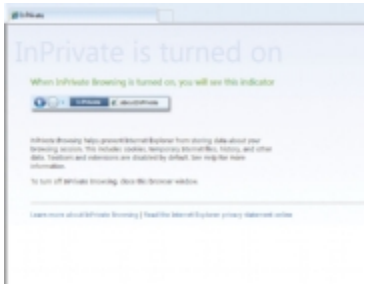
If you've connected with someone on Facebook, LinkedIn, Twitter, or another social network, it's probably because you know and trust the person. Attackers, however, can take control of your friend's online persona and then exploit that trust.

Beware of scams sent from 'friends': Attackers can hijack one of your online buddies' social networking accounts through malware, phishing scams, and other techniques, and then use the stolen accounts to spam you, steal your personal data, or even con you out of cash. Once the thieves have locked your friend out of the account, they may send you a note saying, "Help! I'm in London and my wallet was stolen. Can you wire me some money for a plane ticket?" Or they may recommend that you click on doctored links that will allow them to infect your computer or compromise your own account.

Web Snooping

Now that so much entertainment, shopping, and socializing has shifted online, every Internet user leaves a rich digital trail of preferences. The books you read, the movies you rent, the people you interact with, the items you buy, and other details constitute a gold mine of demographic data for search engines, advertisers, and anyone who might want to snoop around your computer.

Do business with companies you trust: Stay aware of the privacy policies of the Websites and services you interact with, and restrict your dealings to those that you believe you can trust to guard your sensitive information.



Use private browsing: The current versions of Internet Explorer, Firefox, Safari, and Chrome include private-browsing modes. These features, such as IE 8's InPrivate Browsing and Firefox 3.5's Private Browsing, ensure that the site history, form data, searches, passwords, and other details of the current Internet session don't remain in your browser's cache or password manager once you shut the browser down. By protecting such information on the computer you do your surfing on, these features help you foil nosy coworkers or relatives.

Scareware

You're probably familiar with the garden-variety phishing attack. Like a weekend angler, a phisher uses bait, such as an e-mail message designed to look as if it came from a bank or financial institution, to hook a victim. Scareware is a twist on the standard phishing attack that tricks you into installing rogue antivirus software by "alerting" you that your PC may be infected.

Don't take the bait: Stop and think. If, for instance, you don't have any security software installed on your PC, how did the "alert" magically appear? If you do have a security utility that identifies and blocks malicious software, why would it tell you to buy or download more software to clean the alleged infection? Become familiar with what your security software's alerts look like so that you can recognize fake pop-ups.

Don't panic: You should already have antimalware protection. If you don't, and you're concerned that your PC may in fact be infected (not an unreasonable concern, given the existence of a rogue "alert" on your screen), scan your system with Trend Micro's free online malware scanner, HouseCall, or try running Microsoft's Malicious Software Removal Tool; for more help, see "Additional Security Resources." Once you complete that scan, whether it discovers anything or not, find yourself a reputable antimalware app and install it to protect your PC in the future.

Update your browser: Such fake messages will prompt you to visit the scammer's Website, which may infect your system further. Current versions of most Web browsers and many Internet security suites have built-in phishing protection to alert you to sketchy sites. It's important to note that while the databases these filters use are updated frequently to identify rogue sites, they aren't fail-safe, so you should still pay attention to any URL that you consider visiting. To make this easier, both Internet Explorer 8 and Chrome highlight the real, or root, domain of the URL in bold so that you can easily tell whether

you're visiting, say, the genuine *www.pcworld.com* or a spoofed site like *www.pcworld.com.phishing-site.ru*.

Trojan Horse Texts

Some attackers will send spam text messages to your mobile phone that appear to be from your network provider or financial institution. These Trojan horse text messages may direct you to a malicious site or request permission to install an update that will change the settings on your cell phone to allow the attackers to capture usernames, passwords, and other sensitive information from your device.

Go to the source for updates and news: If you receive a text message that appears to be from a trustworthy source, but it directs you to install or update software, or if it initiates the installation and requests permission to continue, immediately exit the text-messaging app and contact the customer service department for the wireless provider or business in question to verify whether the software is legitimate.

You may receive a lot of unsolicited e-mail from companies that you do business with--e-mail that you might even regard as spam--but reputable companies will not send you unsolicited links and updates via e-mail. Similarly, reputable companies will not send unsolicited text messages to your mobile device directing you to install an update or download new software.

Attackers prey on your tendency to trust your wireless provider or financial institution. Do not blindly accept software updates or download applications to your mobile phone simply because the text message appears to be official. If in any doubt, follow up with your wireless provider or with the business.

Lost Laptops, Exposed Data

The portability of laptops and cell phones is convenient, of course, but that same portability means that such devices are easily lost or stolen. If your laptop, netbook, phone, or other device falls into the wrong hands, unauthorized users may access the sensitive data that you've stored there.

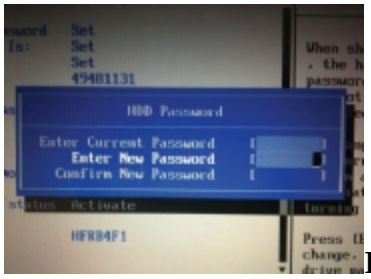
Encrypt your data: You can use a utility such as Microsoft's BitLocker to encrypt data. Unfortunately, BitLocker is available only for Windows Vista and Windows 7, and even then it's exclusive to the Ultimate and Enterprise editions of those OSs (and is also available in Windows Server 2008); you won't find the tool in the consumer versions of Vista and Windows 7.

Fortunately, BitLocker isn't the only game in town. You can use another encryption program, such as TrueCrypt (available for free under open-source licensing), to protect your data from unauthorized access.

Encrypting your data is not without a pitfall or two, however. The biggest issue is to ensure that you always possess the key. If you lose your encryption key, you will quickly discover just how good encryption is at keeping out unauthorized users.

Use stronger passwords: If encrypting seems to be more of a hassle than it's worth, at least use strong passwords to protect your PC. Longer passwords are better; more characters take longer to crack. You should also mix things up by substituting numbers and special characters for letters. For example, instead of using the plain "PCWorldMagazine", you could use "PCW0r1dM@g@zin3". Though that's still a phrase you can easily remember, the character diversity makes it significantly harder to guess or crack.

You should have a secure password to log in to your user account even if you're the only person who uses your computer. Note, however, that while strong passwords are a great deterrent, they aren't impervious to attack: An invader who has physical possession of your computer can find ways to get around that protection.



Lock down your BIOS: By implementing a BIOS password or a hard-drive password (or both), you can ensure that no one else can even boot the computer. Getting into the BIOS varies from system to system. The initial splash screen that your PC displays usually tells you which key to press to access the BIOS settings; watch as the computer is booting, and press Del, Esc, F10, or whichever key it specifies.

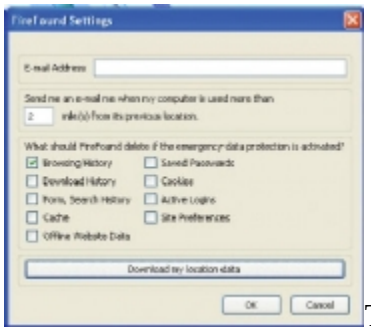
Once inside, find the security settings. Again, these settings vary from vendor to vendor, but the BIOS settings are fairly rudimentary. Learn more about accessing and navigating your system's BIOS in "Tweak Your PC's BIOS Settings the Safe Way."

You can set a master password that prevents other people from booting your computer or altering the BIOS settings. This option goes by different names, but it is often called an administrator password or supervisor password. If you wish, you can also set a hard-drive password, which prevents any access to the hard disk until the password is entered correctly.

Methods for circumventing these passwords exist, but having the passwords in place creates another layer of security that can help to deter all but the most dedicated attackers.

Use a recovery service: If your equipment gets lost or stolen, you'd like to recover it; but if you can't get your hardware back, you'll at least want to erase the data it holds. Some vendors, such as HP and Dell, offer services that try to do both for select laptop models.

Both HP's Notebook Tracking and Recovery Service and Dell's Laptop Tracking and Recovery are based on Computrace from Absolute Software. When you report that a laptop protected with one of these services has been lost or stolen, a small application running in the background on the PC waits for the computer to connect to the Internet and then contacts the monitoring center to relay location information for finding the machine. If a protected lost or stolen laptop cannot be retrieved, or if the data on a system is highly sensitive, these services allow you to remotely erase all of the data stored on it.



Though less comprehensive, free utilities such as the FireFound add-on for Firefox provide similar capabilities. You can configure FireFound to automatically delete your passwords, browsing history, and cookies following a failed login attempt.

Mobile phones can hold a significant amount of sensitive data, too. Fortunately, services such as Find My iPhone, part of Apple's $99-per-year MobileMe service, and Mobile Defense for Android-based smartphones perform similar feats of location tracking and remote data wiping for smartphones. Both MobileMe and Mobile Defense can use the built-in GPS capabilities of your smartphone to pinpoint the current location of the device and relay that information back to you.

Rogue Wi-Fi Hotspots

Free Wi-Fi networks are available almost everywhere you go. Attackers, however, sometimes set up a malicious open Wi-Fi network to lure unsuspecting users into connecting. Once you have connected to a rogue wireless network, the attacker can capture your PC's traffic and gather any sensitive information you send, such as your usernames and passwords.

Verify the network's name: If you want to connect to the Internet at a coffee shop or in another public place, find out the SSID of the establishment's network. The SSID is the name of the wireless network; it is broadcast over the airwaves so that your computer can detect the network, and as a result it's the name that appears in your system's list of available networks.

The SSID for a network at a McDonald's restaurant, for instance, might be "mickeyds." An attacker could set up a rogue wireless router in the vicinity of the McDonald's location and set its SSID to "mcdwifi" or "mickeyds2." Your computer would then display both names on the list of available networks--and the rogue wireless network might even have a

stronger signal and appear higher on the list. Make sure that you connect only to the official network.

When in doubt, don't trust any open network. Most free wireless networks are unencrypted--and therefore unprotected. That means that the data traveling between your computer and the wireless router is susceptible to being intercepted and viewed by other parties that happen to be within range of the wireless network. Unless you have your own secure connection, such as a VPN (virtual private network) connection to the network at your office, you should avoid using public Wi-Fi for logging in to sensitive accounts (such as your e-mail or bank account); instead, limit your Internet usage in such public places to reading the news or checking for weather updates and traffic reports.

Weak Wi-Fi Security

If you're cautious, you've already secured your wireless network with a password to keep outsiders from accessing it or using your Internet connection. But password protection alone may not be sufficient.

Use stronger encryption: Several types of Wi-Fi network encryption are available, and there are some important differences between them. WEP (Wired Equivalent Privacy) encryption is the most common variety employed on wireless networks. If you have a WEP password in place on your Wi-Fi network already, you've taken a significant step toward protecting it from intruders.

But WEP can be easily cracked: Tools are available that allow even unskilled attackers to crack the code and access your network in a matter of minutes. WEP is still helpful, since most aspiring wireless-network hijackers are not dedicated enough to take the time to break in, but to be safe you should use WPA (Wi-Fi Protected Access) or its successor, WPA2. These encryption types resolve the weaknesses of WEP and provide much stronger protection.

Log in to your router's console and find the wireless-security settings. There, enable encryption and select either WPA or WPA2. Enter a password, save the settings, and restart your router--and you'll start surfing more safely.

Endangered Data Backups

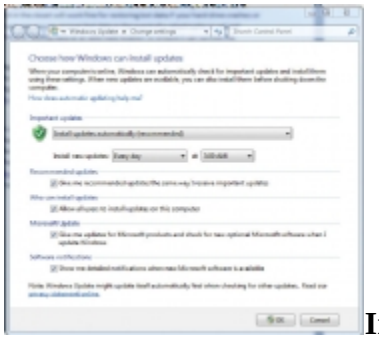
You know that you should back up your data, especially files of irreplaceable items such as family photos, regularly. But while storing backups on an external hard drive or burning them to blank CDs or DVDs and keeping them in the closet will enable you to restore files easily if your hard drive crashes or corrupts, that approach also creates a portable--and thus easily lost or stolen--archive of your sensitive data.

Encrypt your backup data: Be sure to use a backup utility that allows you to protect your data with encryption, or at least a password, to prevent unauthorized access. If you want to take things a step farther, you can put your backup files on an encrypted external USB drive such as the Seagate Maxtor BlackArmor, a PCWorld Best Buy. You can also find external drives with biometric fingerprint scanners, such as the Apricorn Aegis Bio or the LaCie d2 Safe. (For reviews of these drives and others, see "Encrypted Drives Keep Your Files Safe.")

Use an online backup service: If you prefer, you can use an online storage service such as Microsoft Windows Live SkyDrive, which provides 25GB of storage space for free and offers a measure of security by requiring a username and password for access. Unfortunately, copying 25GB of data and keeping it updated via SkyDrive can be a time-consuming and cumbersome process. For a small fee, though, you can use a service such as Mozy, which includes tools to automate the process and to ensure that your data is backed up regularly.

Unpatched Software (Not Just Windows)

Microsoft's products have long been favorite targets for malware, but the company has stepped up its game, forcing attackers to seek other weak links in the security chain. These days, third-party products such as Adobe Reader provide attackers with alternative options for hitting your PC.



Install all security updates: You should have both a firewall and an antimalware utility protecting your system, but one of the simplest--and most effective--ways to guard against attack is to make sure that you keep your operating system and applications up-to-date.

Attackers have discovered that a considerable number of third-party applications such as Adobe Reader and Adobe Flash are present on virtually every computer and contain exploitable weaknesses. To guard against threats, you can use a program such as the Secunia Personal Software Inspector to scan your system, identify applications that have known vulnerabilities, and install the necessary updates.

Do your best to stay informed of existing flaws for the various applications you use, and apply appropriate patches as soon as possible. The About.com Antivirus Software site is a good resource to use in collecting such information. You can also check sites such as McAfee's Avert Labs Threat Library for the latest news on emerging threats.

Though attacking third-party products may be a path of least resistance, bad guys haven't given up entirely on Microsoft products. Windows users should have Automatic Updates (or Windows Update) enabled and set to download and install important security updates automatically. The automatic updates will keep the Windows operating system--as well as other Microsoft software such as Internet Explorer and the various Office applications--patched and current.

5 Security Myths

Think you're doing everything you need to do to be safe? Think again. Here are five common myths about digital security.

Illustration by Frank Stockton

I don't have anything an attacker would want.

Average users commonly believe that the data on their computers is valuable only to them or has no intrinsic value at all, and that therefore they have nothing to protect and no need to worry. There are three problems with this way of thinking. First, instead of pilfering data, attackers often want to take control of the computer itself, as they can employ a compromised PC to host malware or to distribute spam. Second, you may not think that your PC has any important or sensitive information, but an attacker may be able to use seemingly trivial information such as your name, address, and birth date to steal your identity. And third, most attacks are automated and simply seek out and compromise all vulnerable systems; they do not discriminate based on a target's value.

I have antivirus software installed, so I am safe.

Antivirus software is an absolute necessity, and it's a great start, but installing it won't protect against everything. Some antivirus products are just that--they don't detect or block spam, phishing attempts, spyware, and other malware attacks. Even if you have a comprehensive security software product that protects against more than just viruses, you still must update it regularly: New malware threats are discovered daily, and antimalware protection is only as good as its last update. Keep in mind, as well, that security vendors need time to add protection against emerging threats, so your antimalware software will not guard you from zero-day or newly launched attacks.

Security is a concern only if I use Windows.

Microsoft certainly has had its share of security issues over the years, but that doesn't mean that other operating systems or applications are immune from assault. Though Microsoft products are the biggest target, Linux and Mac OS X have vulnerabilities and flaws, too. As alternative OSs and Web browsers gain users, they become more attractive targets, as well. Increasingly, attackers are targeting widely used third-party products that span operating systems, such as Adobe Reader.

My router has a firewall, so my PC is protected.

A firewall is great for blocking random, unauthorized access to your network, and it will protect your computer from a variety of threats; but attackers long ago figured out that the quickest way through the firewall is to attack you via ports that commonly allow data to pass unfettered. By default your firewall won't block normal traffic such as Web data and e-mail, and few users are comfortable reviewing firewall settings and determining which traffic to permit or block. In addition, many attacks today are Web-based or originate from a phishing attack that lures you into visiting a malicious Website; your firewall cannot protect against such threats.

Since I visit only major, reputable sites, I have nothing to worry about.

You certainly increase your system's odds of being infected or compromised when you visit the shady side of the Web, but even well-known Websites are occasionally infiltrated. Sites such as those for Apple, CNN, eBay, Microsoft, Yahoo, and even the FBI have been compromised by attackers running cross-site scripting attacks to gather information about users or to install malicious software on visitors' computers.

Additional Security Resources

Many sites and services on the Web can help you learn more about computer security threats or can analyze your machine to make sure it is clean and safe.

Hoax Encyclopedia: The About.com Antivirus site has a comprehensive database of e-mail and virus hoax messages. Before you forward the next "urgent" alert to your family and friends, check for it on this list.

McAfee Virus Information Library: McAfee maintains a complete listing of malware threats, including details on how they spread and how you can protect your computer against them.

Microsoft Consumer Security Support Center: On this page you can find solutions to common security problems, as well as links to other information and resources for Microsoft's security products.

Microsoft Malicious Software Removal Tool: This tool is designed to scan for and remove current, pervasive threats. Its scan is smaller and faster than a complete antimalware scan, but it identifies only a handful of threats. Microsoft releases a new version of the tool--along with regular security fixes--on the second Tuesday of each month ("Patch Tuesday").

Microsoft Security Essentials: This free antivirus application provides real-time protection for Windows PCs against viruses, worms, spyware, and other malicious software.

PhishTank: A community project, PhishTank is a database of known phishing sites. You can search the database to identify phishing sites, and you can add to the list any new sites you've encountered.

Trend Micro Housecall: Trend Micro's free HouseCall service scans your computer online to discover and remove any viruses, worms, or other malware that may be residing on it.