



Protect Your Family Against Today's Internet Threats

Security Advisor Team
September 2007

A Dangerous Landscape

Everyone spends more time online. You may send an e-mail to a long-lost friend, catch up on work, shop, pay bills, trade stocks, or share photos of your latest family trip. And your kids are online too. Teens are busy on their favorite social networking site, instant messaging, doing schoolwork, and shopping. Even pre-teens are getting into the act with gaming sites and virtual worlds designed just for them. And anyone in the family could use a public computer or Internet connection at the library, coffee shop, or airport.

As the Internet has become convenient to your family's daily activities, it has become highly profitable for criminals. While much media attention has been focused on the perils of kids meeting strangers online or stumbling onto porn, there are other grave dangers, such as identity theft, fraud, or having your PC used to harm others – if you do not take some easy steps to protect your family.

Internet crime is big business. A decade ago, writing harmful software was largely driven by individual hackers' desire for recognition. Today, profit is the clear motive. Organized groups of criminals create the tools and the distribution mechanisms for a wide variety of harmful software that can be used in criminal enterprises. Many of these groups, which are located mostly in Eastern Europe and China, are well organized and run like legitimate software businesses.

Their software perpetrates harm well beyond offensive photos or annoying pop-up ads. They can watch what you and your kids do on the Internet, and they can potentially sell that information to unscrupulous marketers and criminals. They can steal your passwords, draining your bank account or running up your kid's online gaming bill. They cripple the websites of organizations they don't like – and use your PC as part of the attack.

Identity theft has reached record levels. Almost 3.25 million Americans discovered that their personal information has been used to open credit card accounts, according to the Federal Trade Commission (FTC).¹ The Privacy Rights Clearinghouse, a watchdog organization, reported that 159 million records containing sensitive personal information have been involved in security breaches since 2005.² Since companies have only been recently required to report security breaches, the actual numbers are likely much higher.

The analysis provided in this report is based on incident information from the CA Security Advisor team, submitted by CA customers and consumers, as well as public information. The report is intended to inform consumers of the newest and most dangerous Internet threat trends and to offer some practical steps that you and your family can take to protect your privacy.

Malicious Software is a Business

Malware has emerged as a business. Much like legitimate software businesses, there are organizations that develop malware and others that distribute malware to willing buyers around the world. There are toolkits that allow other developers to customize the malware for their purposes. Malware developers have begun to adopt many of the same practices used by legitimate software developers, including developing modular code. Some of these organizations even offer support plans for their malware.

¹ "Identity Theft Survey Report," Federal Trade Commission, September 2003

<http://www.ftc.gov/os/2003/09/synovatoreport.pdf>

² "A Chronology of Data Breaches," Privacy Rights Clearinghouse, <http://www.privacyrights.org/>

Cyber-criminals change their tactics quickly to evade detection by the security industry. For example, image-based spam exploded late last year and early in 2007, as spammers found that embedding their fraudulent offers and links to harmful websites into images would allow them to slip past anti-spam filters. But as security vendors became more adept at catching image-based spam, the criminals moved onto using attachments, such as PDFs, Word, and Excel files, to evade spam filters in the hopes that you'll respond.

Cyber-criminals use all of the tools at their disposal to accomplish their purpose. They have recently moved to a phased approach to getting their malware on your computers. Security experts call this "multi-component malware." Here's one scenario showing how it can work: An attacker sends you spam, using consumers' computers that have been taken into a botnet. The spam email contains a link, which, if clicked on, takes you to a fraudulent website. If you're using a browser that isn't up-to-date, you may be vulnerable to malicious software that can be downloaded onto your computer, even without your knowledge, merely by visiting the website. Once executed on your computer, malware can watch which websites you visit, and communicate that information to an unseen party. It can download a different kind of harmful software every day.

For the criminal, multi-component malware gives them great flexibility to change and fine-tune their attacks. It also enables malware to do much more, because the many components perform different functions. And the more criminals change their *modus operandi*, the harder it is for security software to find and remove them.

Botnets³ are another serious problem, especially for home computers that do not have protected

connections to the Internet. Millions of people's PCs are controlled by botnets. The botnets are a way for criminals to use PCs without their knowledge. Criminals can rent a botnet from its owners (who are called bot-herders). These computers are networked together, so that the attacker is able to combine bandwidth to launch distributed denial of service attacks, which can cripple websites, and processing power for tasks such as cracking passwords. They may use botnets to send viruses, trojans, spam, or other harmful software to others on the Internet. By compromising consumers' unprotected computers, the criminals can also prevent counterattacks because of the large number and variety of IP addresses used by the botnets.

Today bot-herders rent their botnets by country or geographical region, but as they collect more information about their victims' behavior, it's not inconceivable that they would offer targeted, demographic-based marketing that would rival the largest legitimate marketers. Imagine how marketing campaigns or political campaigns can turn in the hands of this criminal underground.

Protect Those at Risk

In this Internet age, you may marvel at your kids' multitasking ability: they text on their cell phones, hang out on their favorite social networking sites, and instant message, all while rolling their eyes at you. Kids are often doing more online than their parents realize. They're often more skilled at using computers and the Internet, which can cause them to encounter – both unintentionally and intentionally – pictures, malicious software, and people that you would not condone.

Teens, college students, and young adults are heavy users of social networking sites like MySpace and Facebook, and they are likely to use mobile social networks like Twitter or Dodgeball long before you think it's cool for everyone to locate you by your mobile phone.

³ "Botnet," CA Security Advisor Glossary
<http://www3.ca.com/securityadvisor/glossary.aspx#Botnet>

Parents of pre-teens need to remain alert. Schoolyard bullying has moved to the Internet, where kids can be harassed around the clock on social networking sites and by text messages, instant messages, and e-mail. And virtual worlds and games lure the undivided attention of the under-13 set.

Teens and young adults have grown up with technology as part of the fabric of their lives, and they do not approach it with the same caution you do. They are on the verge of earning income, which increases their value as targets. In fact, the largest group of identity-theft complaints last year came from 18- to 29-year olds, according to the FTC.⁴ The danger is that they generally don't place the same value on protecting their privacy.

People who are newer to using computers, such as seniors or recent immigrants, are also at a greater risk. Ten percent of identity theft complaints last year came from victims 60 and older. They may be unfamiliar with what you consider to be common-sense rules of the Internet, although they have embraced tracing their genealogy or sharing pictures of their grandkids. They may be likely to click on one of the increasingly realistic phishing messages that try to trick them into visiting a fraudulent website and volunteering sensitive information, which can be captured and used to commit fraud and identity theft.

Malicious Software by the Numbers

CA Security Advisor team keeps watch on the latest threats 24 hours a day, seven days a week to protect your family and businesses worldwide. It's clear from even a cursory look at the numbers that Internet threats are changing fast and becoming more severe.

⁴ Identity Theft Victim Complaint Information, Federal Trade Commission, 2006.
http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf

Viruses are the most well-known of the trio of malicious software – viruses, worms, and trojans – but trojans now dominate the landscape. From January to June 2007, CA Security Advisor saw that 65% of the malware submitted by customers were trojans, 18% were worms, 4% were viruses, and 13% were other types of malware.

Most Common Malware

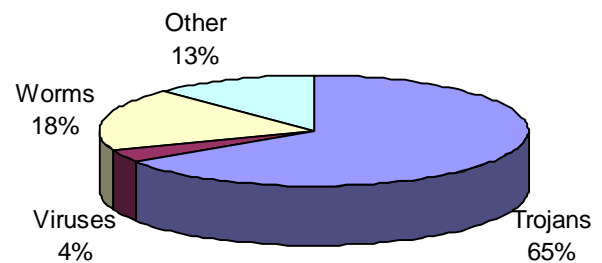


Figure 1: Trojans are the most common type of malware by far. Cyber-criminals have turned to trojans because of their flexibility.

What are viruses, worms, and trojans? A virus is self-replicating code that requires a host (which is usually a file) to “infect.” Viruses may delete files, crash your computer, or cause your computer to act strangely.

Worms can be particularly dangerous as they can spread on their own very quickly across the Internet. Some cripple computers as they go; others drop additional malware or open the compromised computers up to backdoor control by a malicious attacker.

Trojans are a favorite tool of criminals because they are flexible. The term trojan is applied to software that does something that their programmers intended but that the user would not approve of if they knew about it. Unlike worms, trojans can't spread on their own, so criminals use other techniques, such as social engineering or spam, to gain access to computers.

Trojans have a wide variety of functionality. For instance, they can collect sensitive information on affected computers, such as a user's login details and other passwords, and transmit the information to a remote controller. Trojans are often spammed out to users, many of which, like Win32/Sintun and Win32/Pecoan⁵ trojan variants, are widespread this year.

Top Ten Malware			
1.	Win32/Luder	Worm that spreads via email and infection of Windows executables	16%
2.	Win32/Frethog	Online game password stealer	8%
3.	Win32/Stration	Multi-component, mass-mailing worm that downloads and executes other components	6%
4.	Win32/Tibs	Detects Windows executables encrypted with a method known to be associated with Luder, Sinteri, and Pecoan	6%
5.	Win32/Pecoan	P2P file downloader	5%
6.	Win32/NSAnti	Detects files that have been packed with NSAnti packer	4%
7.	Win32/SQLSlammer	Detects log files containing network traffic information that may alert the user to a possible intrusion by SQL Slammer	3%
8.	HTML/Mallar	Detects HTML files been modified by Win32/Mallar, a polymorphic worm that replicates by exploiting Windows vulnerabilities	3%
9.	Win32/Rbot	IRC-controlled backdoor/bot	3%
10.	Win32/Feeb	Spreads by emailing itself, and steals information, such as for online banking or e-commerce	3%

⁵ Win32/Pecoan, CA Security Encyclopedia <http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=60917>

Let's look at some of the more common types of malware that the CA Security Advisor team has seen this year and the damage they can do. The "Top Ten Malware" chart lists the most common malware from January to June 2007.

A few worms have caused widespread damage this year. Win32/Stration⁶ and Win32/Luder⁷ are of particular note. Luder, the #1 malware on the list, was contained in the "Happy New Year" spam that seemed like it was everywhere earlier this year. Luder is a worm that spreads via e-mail and can infect other files. It also drops a trojan that can download and execute other malicious software.

Stealing online gaming accounts can be more profitable than stealing bank accounts. Characters, virtual money, and other goods for online games like World of Warcraft are bought and sold in underground websites that rival legitimate commodity markets. The Frethog trojan (#2 on the Top Ten) is evidence of the big business of stealing gaming passwords. Shady criminals offer stolen game accounts for sale. Frethog is designed to steal passwords and other information relating to online games. With relevant login credentials thus acquired, a criminal can then access and use stolen accounts. Or they can use their malware tools to set up a shop of their own.

The trend toward stealing game-account passwords goes well beyond the technical issues and is clearly one of legal, financial, and social issues. It's difficult for security companies and the authorities to track the activities of these underground groups, many of which operate in East Asian countries such as China. And so far, there have been no penalties for such criminal activities, but as this trend grows and the

⁶ Win32/Stration, CA Security Encyclopedia <http://www.ca.com/securityadvisor/virusinfo/virus.aspx?id=58375>

⁷ Win32/Luder, CA Security Encyclopedia <http://www.ca.com/securityadvisor/virusinfo/virus.aspx?id=61119>

financial losses mount, the legal and criminal penalties will follow.

Stration (#3 on the Top 10) burst on the scene in late 2006, and it continues to be widespread. Stration is a multi-component worm that spreads through e-mail and instant messenger. Its creators have used it for financial gain as they can also send spam from infected computers. An e-mail containing Stration may use one of 15 or more different subject lines, such as an e-mail failing to be delivered or informing you that a worm is being distributed from your computer – seemingly helpful messages that may fool even savvy users.

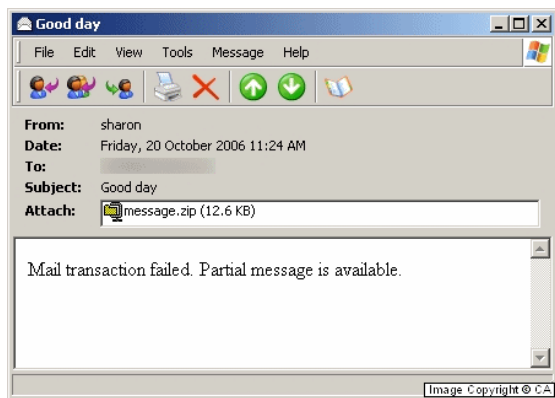


Figure 2: The Stration worm is highly prevalent this year. Stration spreads through e-mail, using such messages as "Mail transaction failed," which may fool even savvy Internet users into clicking on the attachment and unleashing the attack.

Using multi-component malware is just one technique that criminals use to evade detection and removal by security products. The use of packers and encryptors, which work mainly to prevent access to the malware's code, have become widespread. Packers/encryptors such as Tibs (#4 on the Top Ten Malware) have been used by many inter-related pieces of malware, such as Sintun, Sinteri, Pecoan, Singray, and Sinhar. NSAnti (#6 on the list) is another popular packer often used by game password stealers and other malware originating from Asian regions.

Pecoan (#5 on the list) is a family of trojans that establishes communications with a number of

systems on a custom peer-to-peer network. Via this network, Pecoan can download and execute arbitrary files on the compromised system. It can arrive via a number of different delivery mechanisms, including being dropped by the worm Luder or being spammed.

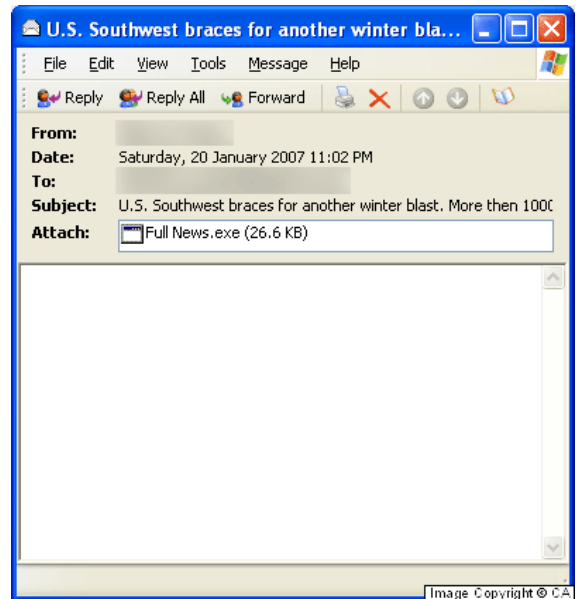


Figure 3: Pecoan is a trojan that spreads via e-mail and the Luder worm. It can execute arbitrary files on compromised computers and establishes communications with peer-to-peer networks.

Spyware by the Numbers

Malware is clearly capable of significant damage and loss, but it's not the only harmful software out there. Spyware is any kind of software that gathers or transmits information about your computer or your behavior online without your knowledge.

Spyware comes in many forms and goes by many names, but trojans once again top the list. (Security experts classify trojans as malware when it has a payload, similar to viruses or worms, and they classify trojans as spyware when the primary activity is to spy on your activities.) Whatever the classification, criminals have clearly shifted their activities to trojans because of their flexibility.

Security experts have seen a significant shift in the types of spyware used. Last year, adware and hijackers were the most common, and this year adware and trojans are now the most common forms of spyware.

Most Common Spyware

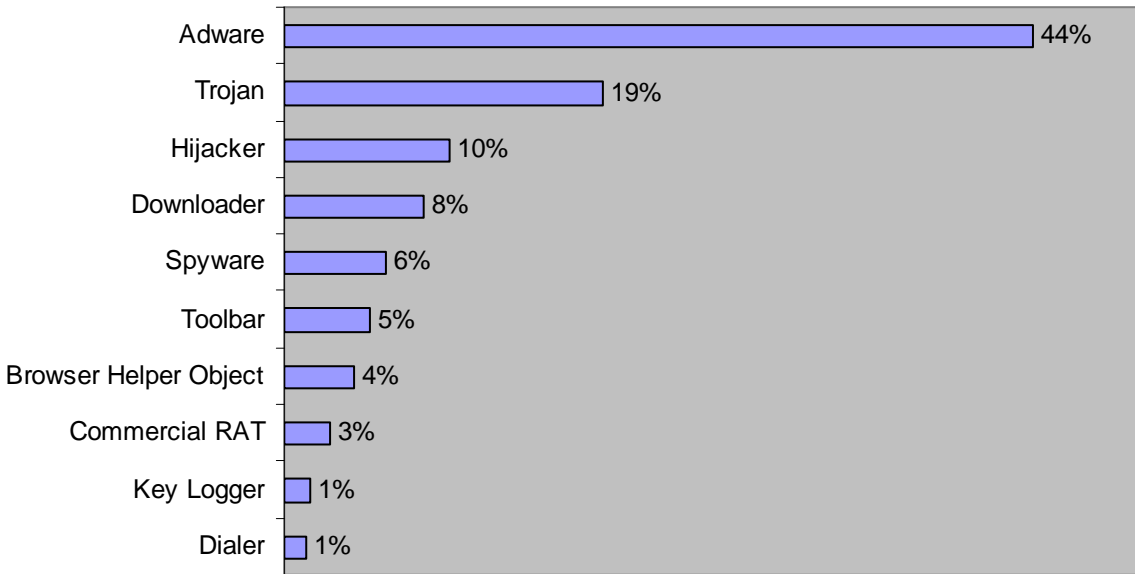


Figure 4: Spyware comes in many forms but in general it gathers or transmits information about you and your behavior without your knowledge. This year, adware and trojans are the most common types of spyware, with trojans overtaking hijackers from last year.

Let's take a look at some of the most common forms of spyware reported by customers over the last 12 months.

- **Adware.** Adware displays pop-up/pop-under ads where the primary user interface isn't visible or that do not appear to be associated with the product. Adware is becoming less common because many of the adware companies have cleaned up their business practices in response to security industry and governmental pressure. Other adware companies have shifted their businesses farther into the grey market of subversive software (and largely became trojans).
- **Trojans.** Trojans and downloaders are often a one-two punch in a multi-component malware

attack. Win32/Nuven was the most common trojan-as-spyware seen this year. Nuven poses as fake applications to download and executes variants of other malware. Nuven usually appears on websites that promote them as applications such as video file-format decoders and applications for obtaining pornography.

- **Hijackers.** Hijacking is a type of network security attack in which the attacker takes control of a communication. In respect to malware, there are many forms of hijackers, including DNS, browser, error, and homepage hijackers. Each

form of the hijacker attacks or takes control of a different type, path, or kind of software. A browser hijacker is a type of malware program that alters your computer's browser settings so that you may be redirected to websites that you had no intention of visiting, such as resetting your home page.

- **Downloaders.** Downloaders can download and may execute or install software without a user's permission. Downloaders are often part of a multi-phased installation. They are popular because they allow distributors to change the malware more readily. Newer downloaders not only distribute spyware, but also defend against their removal. This defense allows criminals to extend the lifespan of the malware that they distribute, since it's harder for the anti-spyware solutions to remove them. Some downloaders can defend against the removal of multiple families of spyware, a "service" which criminals offer for hire.

- **Spyware.** Spyware is any software that employs a user's Internet connection in the background without their knowledge and gathers/transmits info on the user or their behavior. Many spyware products collect information from a user's web browser, IP address, and system information, such as time of visit, type of browser used, the operating system and platform, and CPU speed.
- **Toolbars.** A toolbar is a group of buttons that perform common tasks in a web browser. Toolbars may be created by Browser Helper Objects.
- **Browser Helper Objects.** A Browser Helper Object (BHO) is a DLL module that's designed as a plug-in for Internet Explorer to provide added functionality. For instance, a BHO may allow you to display a file format that the browser can't ordinarily display, reading a PDF file within your browser. The security risk is that a BHO doesn't need any kind of permission to install malicious components and thus spyware may be spread without the user's knowledge.
- **Commercial Remote Administration Tool.** A Remote Administration Tool (RAT) is a trojan that provides an attacker with the capability of remotely controlling a computer.
- **Key Loggers and Password Capture.** Key loggers can record every word you type or send over the Internet. Password capture programs are a type of key loggers. Criminals use key loggers and password capture programs to capture your passwords, account numbers, and other personal information, which they can use for identity theft, fraud, or other illegal activities.
- **Dialers.** A dialer is used to connect to dial-up servers, such as Internet service providers. It allows autodialing, callbacks, and listing of phone numbers.

Another troubling trend is ransomware. A window may pop up on your computer telling you that you have ransomware once your

computer is infected. Or you may receive an email with a Trojan file/ransomware as an attachment. The ransomware may threaten to publish your information online or encrypt the data so you can't use it.

If ransomware is installed on a computer, it can comb through the information on your hard drive and encrypt your data. The e-mail may demand \$200 to \$300, an amount small enough that it seems worth paying to get your data back. But if you do pay, there's no guarantee that your data will be unlocked or that you won't be a victim of future blackmail.

Consumers must also be careful about rogue, or fake, anti-spyware software. Rogue anti-spyware is typically distributed via online ads for free anti-spyware software. You should be aware that some of these programs do in fact contain malware or are simply relatively useless against the majority of spyware threats that exist today. After scaring you into believing that your computer has security problems, the rogue anti-spyware offers to sell the user a license that enables the removal of the supposed problem. After the user pays up, the scheme will either undo the threat it installed or offer no fix at all. Common rogue anti-spyware programs are PestTrap, SpySheriff, SpywareStrike, and WorldAntiSpy.

Most Common Types of Spyware	
Adware	EliteMedia
Trojan	Win32/Nuvens
Hijacker	CnsMin
Downloader	Zlob
Spyware	New.Net.Domain
Toolbar	Mirar
Browser Helper Object	FlashGet
Commercial RAT	VNC
Key Logger	SafeSurfing
Dialer	TrafficAdvance

Software Vulnerabilities by the Numbers

But harmful software isn't your only worry. The software you use every day – your operating system, web browser, Microsoft Office applications, Flash, PDF readers, and your mobile phone – has bugs or security holes. Security experts call security bugs “vulnerabilities” and criminals can use them to plant malicious software or otherwise take advantage of your computer without your knowledge. Vendors work to patch, or correct, these vulnerabilities as they're identified and reported. There's a community of security researchers who work diligently to find new software holes. Some of these researchers have good intentions, and they report the vulnerabilities to the software vendor so they can be fixed. But others look for vulnerabilities that they can use to make a profit – either by selling to hackers or by using it themselves.

In looking at the numbers, software vulnerabilities are on a steady rise. The National Institute of Standards and Technology (NIST), which is a division of the U.S. Department of Homeland Security, maintains the National Vulnerability Database.⁸ In 2006, NIST reported 6,600 software vulnerabilities. From January to June 2007, NIST has reported 3,596 vulnerabilities. At this rate, 9% increase in vulnerabilities will be reported this year.

In this section, we'll look at vulnerability trends in operating systems, web browsers, Flash, Adobe Acrobat, Web applications, social networking sites, and mobile phones.

Microsoft and Apple Operating Systems

Criminals continue to target the family of Microsoft operating systems, simply because so many people use them. Since its release in January 2007, 20 vulnerabilities have been reported in Microsoft Vista®, the operating system Microsoft designed for security. The number of people using Vista is still relatively small, in comparison to other operating systems, but Vista has become a fruitful target of security researchers because of its market positioning as the newest and most secure version of Microsoft Windows.

Windows® XP is still a big target. Many consumers use Windows XP, especially gamers, and XP is a staple of many businesses. It's also important to note that vulnerabilities in Windows XP also generally apply to Vista. NIST reports that Windows XP has 29 newly reported vulnerabilities so far this year. Nineteen of them are high or medium severity, which are the ones that are most important to patch first. At this rate, Windows XP will easily surpass the 55 vulnerabilities reported last year.

Conventional wisdom holds that the MacOS X operating system is more secure than the Windows platform, yet that confidence may crumble when you take a closer look at the numbers. Vulnerabilities are being reported at even a higher rate than the Microsoft platforms. In the first half of this year, NIST reported 51 vulnerabilities in MacOS X, of which 38 were medium or high severity. Last year, NIST reported 104 vulnerabilities in MacOS X, so vulnerabilities are being identified at a slightly higher rate.

Web Browsers

Browsers are one of the most commonly used applications today. Many people believe that Mozilla® Firefox® is more secure than Microsoft Internet Explorer, but their vulnerabilities are on par. In the first half of 2007, NIST reported 52

⁸ The National Institute of Standards and Technology's National Vulnerability Database
<http://nvd.nist.gov/statistics.cfm>

vulnerabilities in Internet Explorer – of which half were medium or high severity. And there were 53 vulnerabilities reported in Firefox – of which almost half were medium or high severity. The numbers are climbing. In 2006, 96 vulnerabilities were reported in Internet Explorer and 103 reported in Firefox.

Even less popular browsers have more security holes. More than double the vulnerabilities have been reported in the Opera browser. NIST reports 14 vulnerabilities this year versus seven last year, and more than half of this year's vulnerabilities are medium or high severity. Apple® Safari® has 19 newly reported vulnerabilities this year – nearly twice the number reported last year, and half of them are medium or high severity.

Flash, Acrobat, and Other Tools

Flash is an increasingly integral part of the Web surfing experience, but running Flash on your computer can put you at greater risk. NIST reported five Adobe Flash vulnerabilities so far this year – up from just one last year.

Security experts have long coached consumers not to open attachments from people they don't know, and savvy Internet users know to avoid clicking on attachments with .exe, .zip and other file extensions. Be cautious when clicking on PDF attachments – just as you approach Word, Excel, and PowerPoint attachments with caution. Spammers have turned to PDF attachments to distribute spam. And criminals have begun to find vulnerabilities in the PDF readers that will allow them to compromise your computer. In the first six months of this year, NIST reported six vulnerabilities in Adobe Reader (which is the same as for all of last year).

The Adobe Acrobat Reader Plug-in, which allows you to view PDFs within a web browser, has five new vulnerabilities reported this year. And even the open-source Foxit PDF Reader has one new vulnerability this year.

Web Applications

You and your family may use a variety of Web applications every day, including webmail, social networking sites, blogs, and discussion forums. Criminals can use security holes in all of these Web applications to trick you into volunteering sensitive information, downloading or launching a malicious program, or otherwise compromising your computer. Cross-site scripting, cross-site forgery, SQL injection and PHP attacks, which we'll describe in this section, may seem arcane to someone who doesn't deal with computer security every day, but they translate into real dangers for you.

A major Web application danger is from cross-site scripting attacks, which is a type of security weakness found in Web applications that allows malicious users to inject code web pages that are viewed by other users. Another danger is a cross-site forgery, which is also known as a one-click attack. A cross-site request forgery is a malicious exploit of websites involving transmission of unauthorized commands from a user the website trusts. The difference is that a cross-site scripting vulnerability relies on a user's trust of a website, while criminals who perpetrate cross-site forgeries take advantage of the trust a website has for you.

SQL injection attacks have long been used, and today apply more than ever to Web applications. SQL injection is a technique that exploits a security vulnerability in a database. Criminals are also increasingly finding and taking advantage of vulnerabilities in PHP, which is a scripting language that's widely used in websites.

Social Networks

While millions of teens use social networks like MySpace and Facebook, they can present real dangers, both technical and social. For instance, MySpace has been under recent fire for being lax about preventing sexual predators from using its site. Would-be attackers can insert themselves

into a social network, gain status, and then subvert that trust for profit.

Social networks are vulnerable to all of the weaknesses that we discussed in the “Web Application Vulnerabilities” section. In addition, their very nature as communication hubs makes them more dangerous. On most websites, the ability to add content or code is generally limited to a small group – the website owner and publisher, but on a social networking site (or a blog or discussion forum for that matter) anyone can add content or code. That means about anyone can add HTML pages – and malicious code. And on a community site, attacks spread faster because everybody and everything is interconnected. So if your MySpace page is modified with exploit code to compromise your friends’ pages, then their friends’ pages are also often eventually compromised.

You can also unknowingly download harmful software from social networking sites. For instance, you may download software to watch videos, but embedded in that software is spyware that will watch your activities or adware that may pop up unwanted ads.

Another growing danger to personal privacy is mobile social services that let people know where you are. Teens and young adults may find it fun to have friends (and friends of friends and strangers) around the world know what they are doing at any given moment (their parents are less likely to want their boss to know they’re at Starbucks when they should be at their desks), but unsavory people can use this information, along with other personal information, for far more chilling purposes than letting your friends know where to meet them.

Mobile Phones

You need to pay increasing attention to your mobile phone. Although the number of reported vulnerabilities is still relatively small, mobile phones are likely to rise in importance as a target. They store personal information. They’re used for Web surfing and e-mail access. And in

the not-to-distance future, they will be used to make purchases.

NIST reports two vulnerabilities identified in Microsoft Windows Mobile so far this year. Windows Mobile was released earlier this year, and as it is used on more mobile phones, we expect to see a rise in the number of vulnerabilities reported, as is commonly the case with new operating system releases.

Bugs are being reported in the new Apple iPhone as well, including one that hackers can use to retrieve data from an iPhone by tricking a person into visiting a malicious website.

Ways to Keep Your Family Safe

Internet dangers are growing, but you don’t have to unplug your Internet connection, quit your e-commerce habit, recycle your cell phone, or generally become a Luddite. Protecting your privacy and safety on the Internet is a two-step process. First, let the security technology work for you. Security vendors watch threats develop minute-by-minute around the world, and they work diligently to develop new protections against the latest threats. Use the security technologies they develop, and above all, make sure you keep all of your software up-to-date.

Second, make sure your family follows common-sense guidelines when using the Internet. Staying safe on the Internet also means that everyone in your family should surf responsibly and not engage in risky Internet behavior.

Let the Technology Work For You

Here are some easy steps you can take to let the security technology protect you.

- 1. All computers in your house should be protected with good antivirus, anti-spyware, and anti-spam software.** Many

security vendors integrate these security capabilities into a single software suite, which is an easy way to get complete protection. Up-to-date antivirus software is your first line of defense against viruses, worms, and trojans. Anti-spyware programs can keep intruders from watching your activities on the Internet and stop adware, spyware, key loggers, and other forms of malicious software. Anti-spam software can eliminate volumes of junk mail, phishing attacks, and suspicious e-mail attachments.

- 2. Use a personal firewall.** Your computers should also have personal firewalls, which protect them against intrusions and malicious software. Personal firewalls can also control which applications access the Internet and control cookies that track your behavior on the Internet, among other capabilities.

Some games conflict with personal firewall settings, so the gamers in your household may turn off personal firewalls. This is extremely dangerous, as it may allow password-stealing trojans a free pass into their computers. Do the extra configuration work to make sure the online games work with the personal firewall. It's well worth the effort.

- 3. Secure your network router.** The network router is your gateway to the Internet, so make sure you use a router that has built in firewall functionality. You should also configure it securely, including changing the default password to one that can't be easily guessed. Make sure that not just any communication port can connect to the Internet. For instance, many bots use the same communication ports as general Web traffic, so they can't be blocked.

If you are using a wireless router, make sure you change the default SSID and don't broadcast the SSID. Be sure to set up authentication, encryption, and filtering, using WPA2 or WPA, and MAC filtering, so that individuals must enter a password to

use the wireless network and so the wireless traffic is encrypted. If you do not protect your wireless connection, anyone within range can use it. Neighbors may just "borrow" your connectivity, but criminals can also use your Internet connection to send spam, malware, or to attack you directly. If your network connection looks like it's the source of an attack, your Internet provider may temporarily turn off your connection to the Internet, and you might even get a visit from law enforcement officers.

- 4. Keep all of your software updated.** Many people feel confident in their home security routine because they keep their operating systems protected with automatic updates. But that's not enough. It is shaping up to be the worst year on record for Windows XP and Vista vulnerabilities. Internet Explorer and Firefox are running neck-and-neck in vulnerabilities. And the criminals have turned to exploiting vulnerabilities in software you depend on but give little thought to, such as Acrobat and Flash.

To stay protected, you must keep all of your software, including your web browser, Office applications, Acrobat, Flash, and browser plug-in tools current with the latest patches. Installing vendor patches as soon as they come out is critical to protect you against the latest threats. Use automatic updates where possible, so you always have the latest protection.

Having the latest browser software is critical as the browser has become such an important part of using the computer.

If your computers use very old operating systems, consider upgrading to the latest supported editions. For instance, many people still use Microsoft Windows 98, which is nearly ten years old and is no longer supported by Microsoft. Make sure that you're using legitimate, licensed software too, so that you are entitled to these free updates.

- 5. Adjust your browser for increased security.** Set your Internet security settings to high, turn off active content such as ActiveX controls and even Java and JavaScript if you can. Note that while turning off active content like ActiveX and JavaScript can make you safer, it can also adversely affect the quality of your browsing experience. You can also restrict scripting execution on a website by website basis using the NoScript plug-in for Firefox, which is available for free at <http://noscript.net>.

You should also consider using alternative browsers, such as Firefox.

- 6. Backup your data.** This advice is as old as the hills, but laptops are especially easy to steal. Computers in your house could be taken hostage with ransomware if you don't have a protected Internet connection. Use an external hard drive, compact flash, or memory stick, but be sure you regularly back up your data. Encrypt it and protect it with a password too. That way, if the data on your computer is lost or stolen, criminals cannot read through your personal and work information.
- 7. Use an anti-phishing toolbar.** An anti-phishing toolbar such as the NetCraft Anti-Phishing Toolbar⁹ can help to protect you from both suspicious websites and from known malicious websites.

Practice Safe Internet Surfing

Here are some easy steps that you and your family can take to actively protect yourselves against Internet dangers. Security products can protect you, but you also have to do your part.

- 1. Don't open e-mails from people you don't know.** With spam at record levels, exercise caution when opening e-mails. It seems like old advice, but it only takes a moment of inattention to click on a link in spam, which can expose your computer to

malware. Don't open e-mails from people you don't know and be wary of links and attachments in e-mails even if you do know the person. Don't click on links in e-mails. Instead, copy the URL into your browser. These simple practices will protect you against malware-laden spam and phishing attacks. The same goes for attachments: Don't open them unless you are expecting them. You can also configure your email to display in text format (rather than the more graphical HTML) which will provide additional protection.

- 2. Make sure banking, webmail, and financial sites are secure.** When you're conducting online banking or financial transactions, make sure your browser connection is secure. Look for the padlock icon in the lower right of your browser screen, which indicates that you have a secure, encrypted connection. To protect yourself against phishing attacks, it's very important to look at the URL to make sure you're on the site that you think you're on. For example, phishers might change a bank's website slightly to hide their intentions, such as <http://www.example.com/www.yourbank.com/> or <http://www.yourbank.com.example.com>
- 3. Use encryption to protect sensitive data, especially on laptops.** Laptops can be easily lost or stolen, and without encryption, all of your data can be read by anyone.
- 4. Be cautious about instant messaging.** When using instant messaging, think twice about clicking on links in messages. You don't know if your friends' instant message accounts have been compromised by malicious software. Your kids should follow the rules below.
- 5. Avoid P2P networks if possible.** If your kids insist on using P2P networks to download software, music, and games, they should be very careful about what they're

⁹ Netcraft Anti-phishing Tool bar is available at <http://toolbar.netcraft.com/>

downloading. Additionally, gamers should also be very careful when using game cheating software, since these downloads can be bundled with malware.

Downloading, possessing, or using copyrighted music, movies, software, and games is a violation of the Digital Millennium Copyright Act (DMCA). The Recording Industry Association of America (RIAA), Motion Picture Association of America (MPAA), and the Business Software Alliance (BSA) are very serious about protecting copyright and intellectual property rights over music, media, and software. They don't prosecute just the high-profile offenders who copy and/or distribute pirated music, movies, software – they will also go after individuals like you and your kids.

6. **Be wary about letting people you don't know use your computer.** You simply don't know what other people may look for on your computer, which websites they might visit, what browser or system settings they may alter, or what software they may download or install.
7. **When using public computers, be extra alert.** Never complete financial transactions or exchange sensitive personal information when using computers at libraries, coffee shops, airports or other public places. These computers are often already compromised by criminals, or maybe the next person who uses it after you will extract your passwords or other personal information from the browser cache files.
8. **Monitor your children's online activities.**

For the Kids

All members of your household should follow the rules above, but there are a few extra steps that you should take to protect your children.

1. **Tell your children not to respond to messages that are threatening, suggestive, or otherwise make them uncomfortable.** Tell them to report those

messages to you immediately. Watch for signs of cyber-bullying, such as your child being upset after using the PC, and learn how to respond.

2. **Teach your children to protect their privacy.** Kids shouldn't use their real names in chat rooms and when visiting websites. They should never give out their last name, school, or city to people in chat rooms, bulletin boards, or social networking sites. They should never share passwords, even with a friend or someone who claims to be helping them.
3. **Make the Internet a family activity.** Ask your children to show you their online profiles, favorite chat rooms, and friends. Surf the Web with your child, and ask your child about the things he or she did online (and show genuine curiosity). Keep the computer in a family room rather than the childrens' bedrooms.
4. **Install parental controls with Web filtering and optional time restrictions.** Use settings and sounds that activate if a user attempts to access blocked pages too frequently. Consider setting limits for screen time. The American Academy of Pediatrics recommends that parents limit screen time to no more than two hours per day – including television, videos/DVDs, and games.
5. **Explain to your child that not everything they read online is true.** And that not everyone online is who they say they are.

