How to Protect Your Family's PC

A comprehensive guide from the creators of the award-winning ZoneAlarm® Internet Security Suite

Defend The Net !

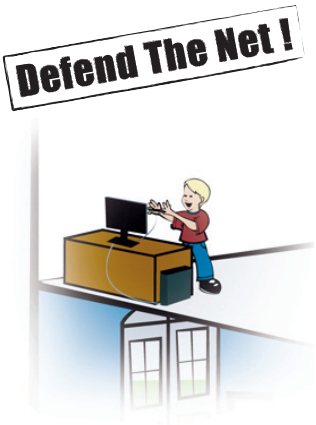
ZoneAlarm® by Check Point®

Defend The Net !

Welcome

ZoneAlarm® by Check Point®

Overview



Protecting Your Family On the Internet

On the Internet, things are not always what they seem.

An e-mail from your bank, asking you to change your online password for security reasons, may actually be a fraud, sent by a criminal hoping to access your account.

A file attached to an e-mail from a friend may be, in reality, a destructive computer virus, sent without your friend's knowledge.

And the 15-year-old girl your teenaged daughter has befriended online could be, in truth, a 45-year-old male child molester.

These are just three examples of the many threats you and your family face on the Internet. Hacker attacks, spyware, worms, identity theft, pornographic spam, privacy intrusions–these, too, are now everyday occurrences online.

Just how risky is the Internet today? Consider the following:

• The number of fraudulent e-mail messages–known as phishing attacks, which are designed to steal critical data (such as bank passwords) from consumers and businesses–increased more than 1,000% from January to June 2005, according to an IBM report. Losses resulting from phishing scams range from $500 million to $1 billion per year, as reported by The Wall Street Journal.

• Eighty percent of users had some form of spyware on their computers in 2004, according to an America Online/National Cyber Security Alliance survey.

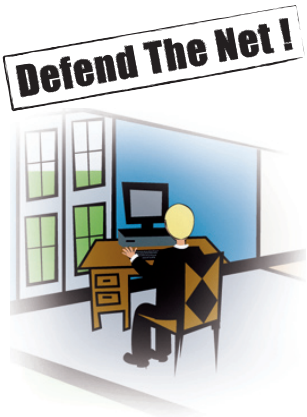
• While yesterday's viruses were primarily destructive, more than half of the major viruses and malicious programs active during July-December 2004 were designed to steal confidential information, according to Consumer Reports.

• Approximately one in five youths aged 10 to 17 have been solicited for sex online, reports a survey from the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention. Fortunately, there are many effective precautions you can take, as well as a variety of computer security tools available. The following is a hands-on, practical guide to protecting yourself and your entire family on the Internet.

Zone Tips:

Parents can help keep their kids secure online into adulthood by teaching them good Internet practices early. Set guidelines and always be aware.

ZoneAlarm® by Check Point®



Starting Off Secure

If you connect an unprotected PC to the Internet, it will be attacked within 15 seconds, according to one industry estimate. While that may seem extreme, the truth is that an unprotected PC–particularly one with an always-on broadband connection–is an easy, desirable target for hackers, identity thieves, and others. After all, a compromised PC has monitary value to a hacker.

Before going online with a new PC, make sure it has, at a minimum, a PC firewall, antispyware, and antivirus software. The software should be fully installed and operational before you begin e-mailing or Web browsing.

The advice is the same if you've had your PC for a while: Install a firewall, antispyware, and antivirus software right away, if you haven't done so already. These programs are designed to block most threats before they can infiltrate your computer. Once installed, perform antivirus and antispyware scans on any hard drives you use (including your computer's internal drive as well as external backup drives). If the software finds viruses or spyware, delete or quarantine them immediately.

Make security scans a routine part of your PC maintenance. Each week, scan your hard drives for viruses, worms, spyware, and any other threats. Also, regularly back up your most important files to an external hard drive, CD, or other storage format, in case your PC's hard drive does get infected or disabled. (See the sidebar "Backing Up Your PC" for details.)

Here, in further detail, are the essential security tools every computer should have:

• **PC firewall.** In architectural terms, a firewall is a fireproof wall that acts as a barrier between one part of a building and another. The firewall's goal: to prevent a fire in one room from getting into another. Similarly, a PC firewall is software that acts as a barrier between your PC and the Internet. The PC firewall's goal: to prevent Internet threats, particularly hackers intent on stealing your personal information or commandeering your PC, from getting into your computer.

Backing Up Your PC

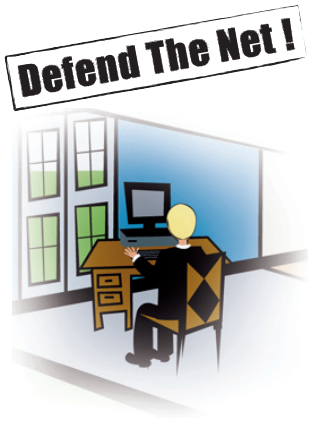
Spyware, viruses, worms, and other Internet threats can wreak almost instant havoc on your computer. Make the mistake of clicking an unknown e-mail attachment, for instance, and a virus could damage, destroy, or make inaccessible your computer files within minutes.

Along with taking security precautions, it's essential to back up your hard drive regularly. Ideally, you should backup each day's work on an external hard drive, a portable USB flash-memory device, or a rewritable CD or DVD. At a minimum, backup your most important files weekly. There are software programs available that automate the backup process for you.

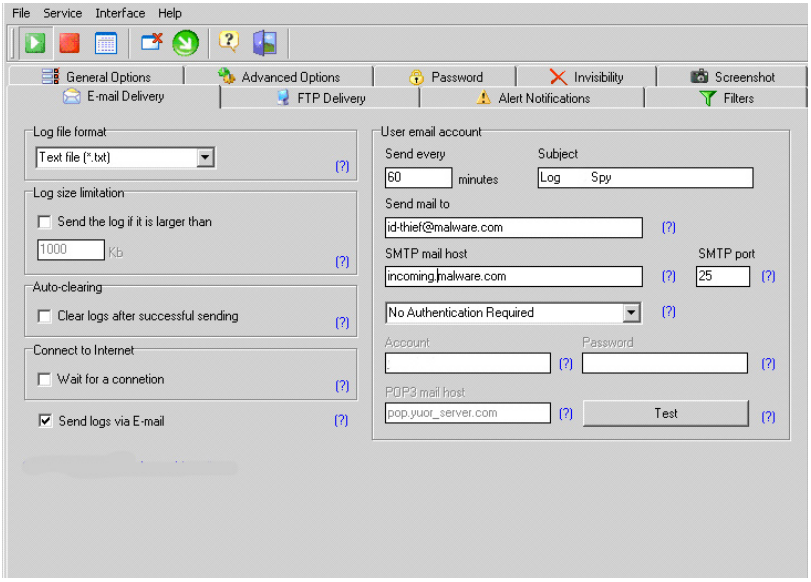
It's also essential to keep a copy of your most important files in an off-site location. That way, if your home or office is damaged in a fire or other catastrophe, your data files will still be safe elsewhere. If it's convenient, store a backup DVD of important files in a bank lockbox.

Once a month, burn a new DVD backup to replace the previous one. Other options: Regularly swap backup discs with a neighbor; keep your backup disc in the trunk of your car, if it's parked away from your home; or back up critical files to an online backup service (though charges apply). Some people even use their MP3 players as backup devices, so their files are always handy.

The bottom line: You've got lots of backup options. Make sure you take advantage of them before it's too late.



A keylogger can be legitimately used by parents to monitor Internet use, but they are also often used by hackers to steal personal information.

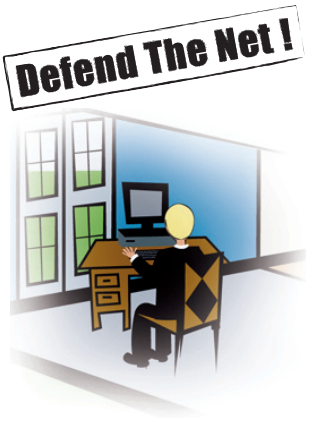


Working in the background, a PC firewall monitors the traffic flowing through your computer to the Internet. When anything seems suspicious, such as a request by an unknown source to connect to your PC, a PC firewall automatically identifies and blocks it. A PC firewall also hides your Internet-connected PC from view, which helps prevent attempted hacker attacks in the first place.

Do you have a home network? If so, many home network routers include a built-in hardware firewall that monitors and blocks inbound communications at the network level. By comparison, the top PC firewalls monitor and block both inbound and outbound communications at the PC level. Combined, a router's firewall and your PC firewall provide desirable multiple layers of protection that a router firewall couldn't provide on its own.

Microsoft's recent upgrade to its current operating system, Windows XP Service Pack 2 (SP2), includes a software firewall, too. **But the Windows XP firewall only protects against unauthorized inbound communications. To safeguard against unauthorized outbound communications as well, you'd need a more robust PC firewall solution.**

ZoneAlarm® by Check Point®



Zone Tips:

A firewall is your first, and often last, line of protection. Don't ever turn it off while connected to the Internet. ZoneAlarm internal tests have shown it takes a hacker less than 8 seconds to detect an unprotected PC.

Some basic PC firewalls can be downloaded free on the Internet. More robust PC firewalls are also available and are often combined with other security tools, such as antivirus, and antispyware in Internet security suites. Such solutions like the ZoneAlarm Internet Security Suite typically cost about $70 with one year of updates.

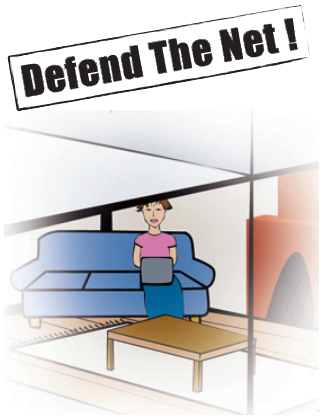
• **Antispyware.** In general, spyware is any software that, without your knowledge or consent, is installed on your computer; gathers data from your PC; transmits that information to others; and/or takes control of your PC. Adware, which exposes you to paid advertisements in pop-up browser windows, can sometimes be considered spyware because it's often installed on your computer without proper consent.

Spyware infections can result from downloading free software programs off the Internet, swapping music files from peer-to-peer (P2P) file sharing networks, and participating in games played with opponents over the Internet. For information on preventing spyware from infiltrating your PC, see the "Staying Secure" section that follows.

Spyware can record everything you type and follow every Web site you visit, then hand that information over to a criminal. At a minimum, spyware can trash your computer, and new strains are capable of repeatedly mutating and resisting removal. That's why every PC should have antispyware protection installed and frequently updated.

There are different approaches to handling spyware: reactive and proactive. Most programs use signatures-which are like fingerprints-to identify spyware on your computer. It uses signatures–which are like fingerprints–to identify spyware that is installed or trying to install itself on your computer. The antispyware will scan for spyware on your system and delete or quarantine it. Proactive spyware technology, like the new OSFirewall™ from ZoneAlarm, is more sophisticated. It blocks most spyware from getting onto your PC in the first place. And it is capable of recognizing and blocking spyware that mutates. For complete protection, make sure your spyware solution is capable of proactively blocking incoming spyware.

ZoneAlarm® by Check Point®



Extending Your Security

Fake e-mails, like this spoofed phishing e-mail: Kids respond to colorful e-mails, and are also more susceptible to contrived warnings from a legitimate-looking source.


Private message from eBay accounts management - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: eBay [aw-confirm@ebay.com] Sent: Mon 9/19/2005 7:38 AM

To:

Cc:

Subject: Private message from eBay accounts management

Security & Resolution Center

eBay Safeharbor Department Notice

Fraud Alert ID : 00626654

Dear eBay member,

You have received this email because you or someone else had used your identity to make false purchases on eBay. For security reasons, we are required to open an investigation on this matter. We treat online fraud seriously and all cases which cannot be resolved between eBay and the other involved party are forwarded for further investigations to the proper authorities. To speed up this process, you are required to verify your personal information against the eBay account registration data we have on file by following the link below.

https://secure.ebay.com/eBayISAPI.dll?action=verify&id=00626654&user=

Please save this fraud alert id for your reference.

When submitting sensitive information via the website, your information is protected both online and off-line. When our registration/order form asks users to enter sensitive information (such as credit card number and/or social security number), that information is encrypted and is protected with the best encryption software in the industry - SSL.

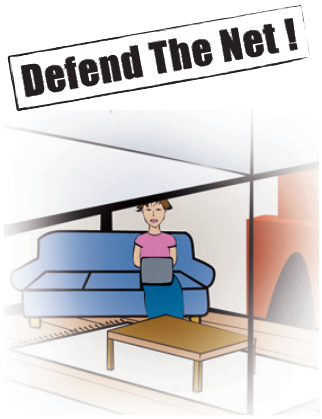
Please Note - If your account informations are not updated within the next 72 hours, we will assume this account is fraudulent and it will be suspended. We apologize for this inconvenience, but the purpose of this

• **Antivirus.** Viruses and worms are programs that spread from one computer to another by inserting copies of themselves into a file or other computer code. Unlike a virus, a worm is self-contained and doesn't need to be part of another program to spread. Typically, viruses and worms infiltrate your PC through e-mail attachments or files you download from the Web.

Viruses and worms can take control of your computer, destroy your files, and render your computer useless. Even worse, some viruses provide a way for hackers to steal your personal information or for spammers to use your computer to spread large volumes of junk e-mail. Antivirus software installed and regularly updated is essential to protecting your PC. And like firewalls and antispyware, there are free antivirus programs available as well as affordable solutions for about $30. Also, antivirus technology is usually included in Internet security suites.

In addition to firewall, antispyware, and antivirus protection, there are other security tools available worth considering. Among them are:

ZoneAlarm® by Check Point®



• **Anti-phishing.** As previously mentioned, phishing is the term used to describe an e-mail that appears to be a legitimate correspondence from a bank, e-commerce site, or other institution but is, in reality, a scam. A phishing e-mail is designed to fool you into providing criminals your credit card number, bank account password, or other sensitive information. Some Internet security suites provide anti-phishing protection. For an example of a phishing e-mail, see "TK" in this document.

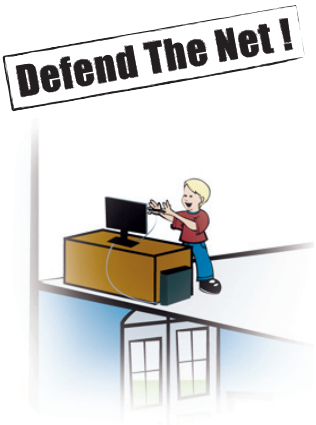
• **Spam blocking.** Junk e-mail, nicknamed spam, fills up your inbox with commercial offers that are dubious at best, fraudulent at worst. If you haven't received an unsolicited e-mail offering cheap mortgage refinancing, Viagra without a doctor's prescription, or replica Rolex watches, you haven't spent much time online. Even worse, spam content is often pornographic. A fall 2005 Consumer Reports survey of its readers found that over 2 million children nationwide had been inadvertently exposed to pornographic spam. Spam blocking or filtering tools are fairly standard now in Internet security suites and e-mail applications. Many Internet Service Providers (ISPs) also offer customers some level of spam blocking.

• **Identity and privacy protection.** Identity theft is a growing problem on the Internet, and your privacy is constantly at stake online because of targeted pop-up ads, cookies that track your Web surfing habits, hackers that attempt to get your PC to transmit your personal data to them, and more. The best PC firewall programs and Internet security suites offer ID and privacy protection controls that protect you from these threats.

• **Instant messaging (IM) protection.** Though seemingly private, IM sessions are vulnerable to hackers, spammers, and online predators. If you or your children use instant messaging, make sure you have IM protection from an Internet security suite or other means.

• **Protection from inappropriate content.** Aside from spam, teenagers and children are frequently exposed to lewd, objectionable, or inappropriate Web content. Just as some cable and satellite systems allow parents to block certain TV channels, some filtering software programs allows you to block Web pages

ZoneAlarm® by Check Point®



Staying Secure

Speeding Up a Slow PC

Has your PC's performance slowed to a crawl? Often, spyware is the culprit. Spyware can monitor everything you type, every Web site you visit. There may be multiple spyware programs installed on your computer. Adware can constantly cause pop-up ads to be displayed. All of these activities cause your PC's performance to suffer.

Unfortunately, some people don't realize spyware (or other malicious software) is their source of their PC's problems—so they solve the problems by purchasing a new system. But there are better, far less expensive solutions.

* Run a complete antivirus and antispyware scan of your system. Quarantine or delete any suspicious files.

* If that doesn't solve the problem, you may need to restore your system to an earlier state. The Windows XP System Restore feature periodically takes a snapshot of your PC to create restore points. Any time an application or driver is installed, Windows XP creates a restore point as well. If a problem occurs, you can literally turn back the clock by opening System Restore and choosing an earlier restore point to return your PC to its earlier, stable state. To find out how to do a System Restore, go to http://www.microsoft.com/windowsxp/using/helpandsupport/learnmore/systemrestore.mspx

* In a worst-case scenario, you may have to reformat your hard drive to get rid of the malicious software and get your computer back in order. While reformatting your drive wipes it clean of malicious software, it also wipes it clean of your files and applications. So you'll need to set aside time to backup your files before reformatting and then to reinstall your operating system, applications and files after reformatting.

Microsoft's Web site includes step-by-step instructions on reformatting your hard drive. The information is online at http://www.microsoft.com/windowsxp/using/setup/expert/honeycutt_02october07.mspx

with objectionable content. Parental control is also a feature in the best Internet security suites.

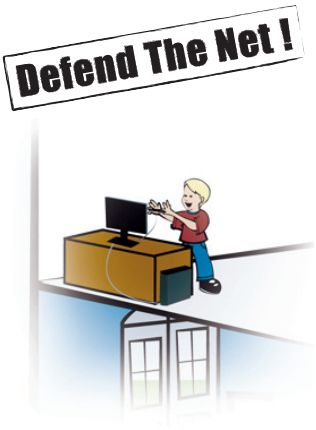
Once you've cleaned your PC of all potential spyware and viruses, and your firewall is preventing hackers from accessing your computer, how do you stay secure? Precaution, awareness, and vigilance are key. Here are some preventative measures that will protect you and your family online.

• **Stay away from peer-to-peer (P2P) file sharing services.** P2P sites allow you to swap and download music files, videos, photographs, and other content, usually for free or at little charge. The original version of Napster, for instance, was one of the most notorious file-swapping P2P services, enabling countless users to illegally swap copyrighted music files.

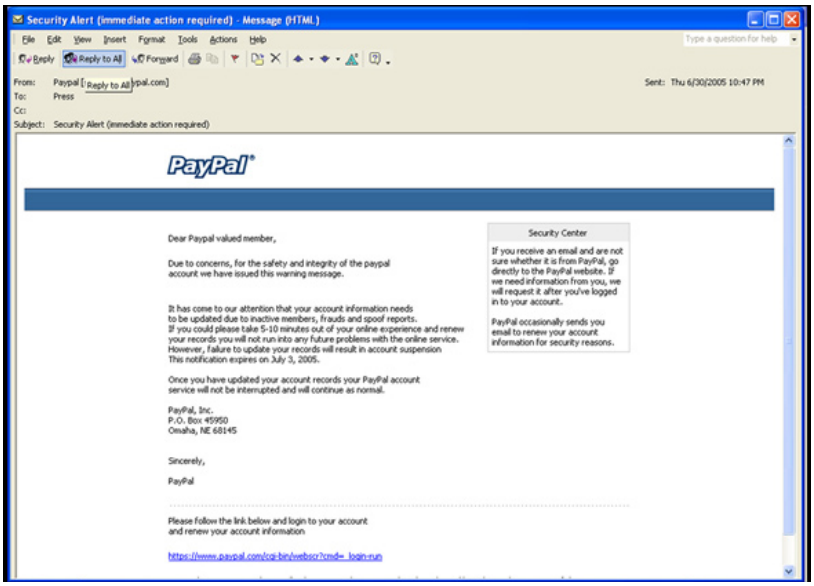
By their nature, many file-sharing services turn your PC into a server, which anyone using the P2P service can access. As you might guess, most P2P services have potential security, privacy-protection, and legal risks. Using a P2P service could make the private information on your computer accessible to others. Some predators have used P2P services to exchange illegal, sexually provocative images of children. And P2P services are notorious for installing spyware and adware on users' computers. Your best bet is to avoid P2P services entirely and discourage your children from using them, too.

• **Be careful playing interactive games.** In order for you to play an interactive game on the Internet, your computer must be identified by a remote server. Once identified, your computer can be targeted by hackers and others, who can then steal your personal data. Before you or your family members play interactive games online, make sure your computer's security software is in full force and has been recently updated.

• **Don't open unknown e-mail attachments.** Viruses and worms often infiltrate computers as files attached to e-mail. When you open the attachment, the virus or worm is activated. Some viruses then propagate by sending themselves as e-mail attachments to everyone in your e-mail address book. To protect yourself (and others), always keep your antivirus software's



Fake e-mails, like the one here (called "phishing"), are often indistinguishable from legitimate marketing e-mails. As are the "spoofed" Web sites they link to. Don't ever click a link in an e-mail to respond to any sort of inquiry. Either visit the Web site directly or call the call a company rep.

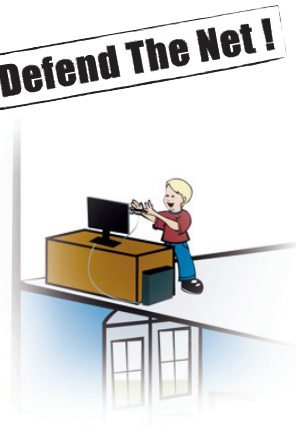


virus definitions updated. Never open an attachment—even from someone you know—that you aren't expecting or that looks suspicious in any way. For instance, if the text of a friend's e-mail seems odd (as if written by a computer, not your friend), the file attached to that message may contain a virus. Make your children aware of viruses and how to avoid them, too.

• **Never respond to spam.** Replying to, or even unsubscribing from, spam only confirms the validity of your e-mail address, which in turn could cause you to get on even more spam lists. Deleting unwanted messages, and using a spam filter, are your safest bets.

• **Never reply directly to e-mail requests for private or financial information.** Though the e-mail from your bank asking you to update your password may look legitimate, it could be a phishing scam. To protect yourself, never reply directly to any e-mail requesting sensitive information. And never click any links in a suspicious e-mail, as they could lead you to fraudulent Web sites. Instead, call the institution requesting the information to verify that the e-mail is legitimate. Or simply open your Web browser and type in the institution's Web site address, where you can log in securely.

ZoneAlarm® by Check Point®



File sharing and peer-to-peer networks can be popular with teens

• **Always look for the lock.** Legitimate banking, e-commerce, and other financial transactions on the Internet are encrypted for security purposes. Encryption means that the information you enter (such as your credit-card number) is translated into a secret code before traveling across the Internet, so it can't be intercepted. Whenever you're on a Web page with encryption, you'll see a lock icon in the bottom right side of the browser window. If you're entering any private data, such as a credit-card number, onto a Web page that does not display a lock icon, stop immediately.

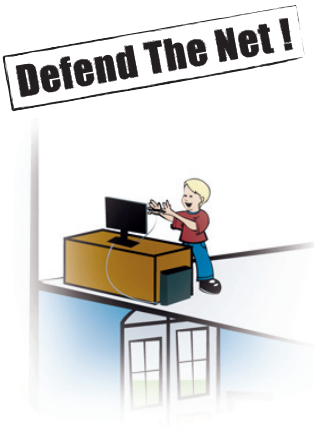
• **Check for the 's.'** Additionally, look at the Web site address for the page you're currently on (it will be displayed in your browser's address line, under the browser toolbars and menus). A secure Web site is designated as "https," rather than the "http" that most Web sites use as an address. The 's' tells you it is a secure Web page.

• **Don't download software from unknown or untrusted sources.** When you download and install shareware or freeware, you may also be inadvertently installing spyware. Also, be aware that some Web sites will prompt you to download a "plug-in." While many of these are legitimate, some can install spyware or adware on your computer. Only download software that you really need, and from reputable sources.

• **Increase your browser's security settings.** Because there are many threats that result from surfing the Web, take a moment to increase your browser's security controls. With Microsoft Internet Explorer, click Tools in the menu bar, then click Internet Options. Next, click the Security tab, then select 'Custom Level' to customize your security settings.

• **Restrict ActiveX controls.** While customizing your browser's security settings, as described above, you'll notice a number of settings relating to ActiveX controls. A set of rules for how applications should share information, ActiveX controls execute some of the interactive elements you see on Web pages. But they also provide access to the Windows operating system on your PC, which can be risky. In the Security Settings dialog box that

ZoneAlarm® by Check Point®



Securing Your Wireless Network

Because they transmit data over radio waves, wireless networks are inherently insecure. Here are some ways you can better protect your home wireless network.

* **Change the default password.** Wireless routers come with factory-set, default passwords for protection, which hackers are familiar with. To stop them from accessing your wireless network equipment, change your router's password.

* **Don't broadcast the SSID.** An SSID (Service Set Identifier) is a name that identifies your wireless network. By default, wireless routers broadcast SSIDs so that you can find and join your network using a wireless device. But you can opt not to broadcast your SSID, to prevent hackers from joining the network, too. Instead, configure your wireless devices to automatically connect to your network's SSID.

* **Use encryption.** Wireless network encryption standards prevent your data from being altered or intercepted during transmission. There are two primary encryption protocols: Wired Equivalency Protocol (WEP), which is the most widely used, and Wi-Fi Protected Access (WPA), which is newer but also more secure. Securing your wireless network with WPA (if your router supports it) or WEP (if it doesn't) helps keep unauthorized users off your network.

* **Keep your wireless hardware's firmware updated.** Manufacturers of wireless network routers often update the security features of the router's internal operational software. Check your device manufacturer's Web site support area regularly to see if a new, free, downloadable security update is available.

* **Secure your PC on a public wireless network.** Public wireless networks, such as Internet cafes, airport lounges, and libraries often have minimal security. In some cases, particularly on wireless networks that are free to use, there is no security at all. An unprotected PC on an unsecure wireless network is especially vulnerable to all the usual Internet risks, such as viruses, as well as some other threats, too. Hackers nearby can monitor your online activities and even redirect you to fraudulent Web sites designed to steal your personal information. Whenever you're on a public wireless network, be sure your personal firewall, antivirus, and antispyware software is running.

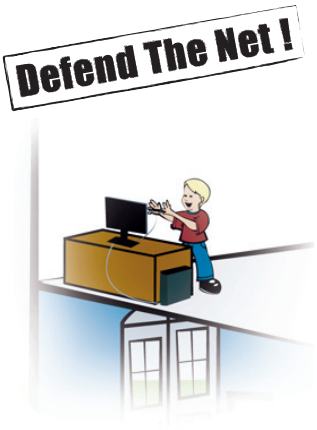
you just opened (see "Increase your browser's security settings," above), select 'Prompt' as the option for 'Download signed ActiveX controls' and choose 'Disable' for 'Download unsigned ActiveX controls.'

• **Consider changing Web browsers.** Because of its vast popularity, Microsoft's Internet Explorer is a frequent target of hackers seeking to exploit the browser's security vulnerabilities. Mozilla's Firefox has become a popular alternative to Internet Explorer, partly because it has had fewer security problems (though it's not immune from them, either). Firefox is a free download at http://www.mozilla.org/

• **Activate automatic Windows updates.** Windows XP allows you to automatically receive patches, updates, and security enhancements to the operating system. Doing so helps keep your computer's security updated and is highly recommended. To turn on automatic Windows updates, open the System icon in the Control Panel (or right-click My Computer and select Properties), and choose the Automatic Updates tab. To check for updates manually, open Internet Explorer and select Windows Update from the Tools menu.

• **Update to Windows XP Service Pack 2.** Windows XP SP2 features a number of security enhancements not offered in earlier versions of the operating system. Updating to XP SP2 can help you stay better protected, though it has its limitations. As previously mentioned, Windows XP SP2 features a PC firewall that protects your computer from unauthorized inbound communications. But unlike Windows XP SP2's firewall, the best PC firewalls protect your computer from unauthorized outbound communications as well. If you're running Windows 98 or an earlier version of Windows, strongly consider upgrading to Windows XP SP2 for its security enhancements (as well as improved stability). For help, go to Microsoft's "Windows XP Home Upgrade Center," at http://www.microsoft.com/windowsxp/home/upgrading/default.mspx

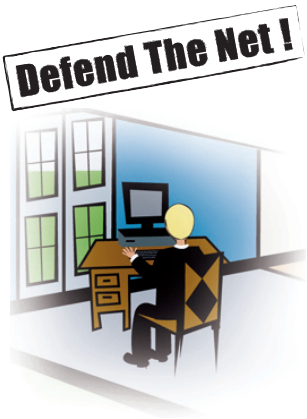
To upgrade to Windows XP Professional, go to http://www.microsoft.com/windowsxp/pro/upgrading/default.mspx



• **Avoid clicking pop-up ads.** Aside from being annoying, pop-up ads can install spyware or adware on your computer. The best PC firewalls and Internet security suites offer pop-up ad blocking, as do many Web browsers and search engine browser plug-ins (such as Google's search toolbar plug-in for Internet Explorer).

• **Secure your wireless network.** Wireless networks transmit data over radio waves, which can be intercepted. As a result, a wireless network is inherently less secure than a traditional wired network. And that means hackers can park outside your home with a wireless laptop and see everything you do on your computer. They can even use your wireless network to commit crimes, such as stealing copyrighted music or uploading child pornography. If you have a wireless home network, turn on encryption using Wi-Fi Protected Access (WPA), if your network router supports it. Older routers may only support Wired Equivalent Privacy (WEP), which isn't as robust as WPA but will still help keep outsiders from piggybacking on your home network.

• **Secure your wireless PC.** When you use a public wireless network, your computer is especially vulnerable. Hackers nearby can eavesdrop on the e-mails you send and Web sites you visit. In what is called an 'evil twin' attack, they can even lead you to fraudulent but legitimate looking Web sites, without your knowledge, and steal your personal information. Whenever you use a public wireless hot spot, make sure your personal firewall software is running and, if possible, refrain from conducting financial transactions.



Protecting the Entire Family

No one is more vulnerable on the Internet than a child or a teenager. As mentioned earlier, minors are often exposed to sexual, hateful, or violent content online, or to material that encourages dangerous or illegal activities. The exposure comes in many forms: spam, Web surfing, chat rooms, even instant messaging.

The dangers don't stop there, unfortunately. Children and teens sometimes unknowingly provide personal information to strangers, which can put them at risk. When minors give strangers their home address, they can unwittingly compromise their entire family's security.

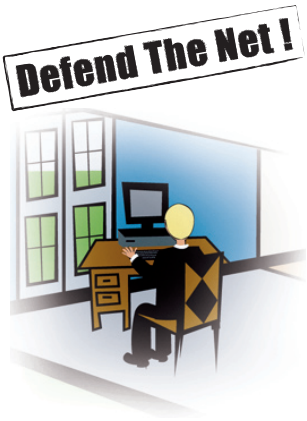
Teenagers sometimes agree to meet people in person they've only communicated with online–which is always risky. Pedophiles have been known to arrange meetings with minors via chat rooms and instant messaging.

Also, children are more likely to open unknown e-mail attachments or do other things online that can expose the family computer to viruses, spyware, and other threats.

Here are some steps you can take to protect your family on the Internet.

• **Educate your children about the dangers**. Encourage your kids to use the Internet for school work, communicating with friends, and to learn about whatever interests them. At the same time, however, teach them about the dangers, just as you taught your child not to talk to strangers or to cross a street without looking both ways. For example, explain to them the importance of not divulging personal information in chat rooms, newsgroups, or anywhere else online. Make them aware what is and isn't appropriate. And if they're old enough to go online, they're old enough to be warned about spyware and viruses.

• **Keep communications open.** Encourage your children to tell you about anything they encounter online that makes them uncomfortable, upset, or confused. Take an active interest in what your child is doing online, without constantly peering over his or her shoulder. The more you appear to be a nosy parent, the more your children are likely to stop telling you about their online activities.



Zone Tips:

Prevention is key. If spyware infects your computer, removing it after the damage is done is not helpful. You must stop it from ever gaining a foothold on your PC. ZoneAlarm's new firewall-based anti-spyware technology prevents spyware and other malicious programs from ever taking control of your PC.

ZoneAlarm® by Check Point®

• **Set specific guidelines and rules.** Create a list of clear, simple, easy-to-understand rules for Internet use. Print the rules and post them near or beside each computer your children use. Consider establishing punishment for breaking those rules, such as a temporary revocation of computer privileges.

• **Know your child's e-mail addresses.** Ask your child or teen for any and all of their e-mail addresses. Find out if he or she has a free Web-based e-mail account, such as one from Hotmail or Yahoo! If so, ask them what they're using it for. You might even ask for their user names and passwords.

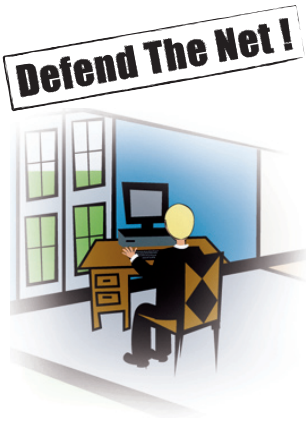
• **Dedicate a computer for your children's use, if possible.** That way, if your kids unknowingly download spyware or viruses, it won't affect your own files and applications stored on the PC. Also, if you have a home network, consider keeping your children's computers off the network, because a malicious program or virus on one computer can spread to others on the same network.

• **Consider keeping the kids' computer in a family room.** If a child has a PC in his or her own room, it's easier for them to do whatever they want, without your knowledge. Placing the computer in a public room may keep your child from straying where he or she shouldn't.

• **Watch for suspicious behavior.** When children quickly change what's displayed on the computer screen when a parent approaches, chances are it's because they don't want the parent to see what they're doing. Keep an eye out for such behavior, as it may indicate your child is 'up to something' online.

• **Keep an eye on the phone bill.** If you're finding unfamiliar charges on your bill, your kids may be making long-distance calls to people they've met online–a potentially dangerous activity.

• **Know the IM lingo.** Often, in instant messaging or in chat rooms and e-mail, kids use acronyms with their online buddies to warn them a parent is nearby. Surprisingly, a whopping 95% of parents couldn't identify common IM and chat room lingo that teenagers use to warn those they're chatting with that their parents are watching, according to a National Center for Missing and



IM Lingo

Want to know what your kids are saying? Here are is some of the most common lingo used in chat rooms and instant messaging:

A/S/L-age/sex/location
BBL-be back later
BF-boyfriend
BRB-be right back
BTW-by the way
CB-ciao baby
F2T-free to talk
FBI-I'll look into it
FYI-for your information
GF-girlfriend
GR8-great
HAK-hugs and kisses
IMHO-in my humble opinion
LOL-laughing out loud
LMHO-laughing my head off
POS-parent over the shoulder
P911-parent nearby or parent alert
ROTF-rolling on the floor
RUOK-are you ok?
TTFN-tah-tah for now

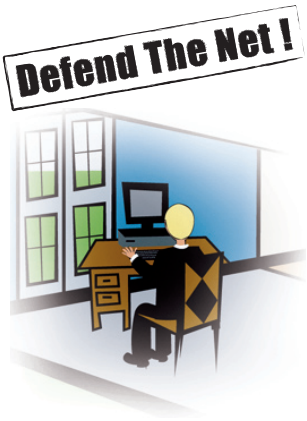
Exploited Children survey. Lingo to watch for includes POS (Parent Over Shoulder) and P911 (Parent Alert).

• **Discourage your kids from posting profiles.** Many chat rooms, bulletin boards, and other online services designed to connect like-minded users encourage you to post a profile. Profiles often give your age, sex, hobbies, interests, and geographic location. These profiles can help your kids meet others with similar interests, but they can also make them a target. To be safe, discourage your children from posting online profiles.

• **Make sure your children use neutral screen names and e-mail addresses.** It's safer if your children create screen names for chat rooms and instant messaging, as well as e-mail addresses, that don't specify age or sex. A 13-year-old girl from Jersey should not use a screen name such as "JerseyGirl13," for instance. A better screen name would relate to a hobby or interest, such as "IPodder04," which suggests the child's been an IPod fan since 2004.

• **Teach kids how to spot predators.** You don't want to scare your kids, of course, but you do want to raise their awareness about child molesters who frequent chat rooms, bulletin boards, and such. Teach them to watch for the warning signs: inappropriate questions about the child's physical appearance, parents (such as questions about how much time the parents spend at home or how closely the child is supervised); expressions of affection; and so on.

• **Use Web filtering tools.** Some software programs are designed specifically to let parents block certain types of Web content. For example, you can block entire Web site categories, such as e-commerce, news groups, software downloads, and more. Some programs allow you to block Web content by keywords, such as 'XXX,' 'alcohol,' and 'gambling.' The blocking controls are password-protected, so your kids would have to know your password to gain access to the controls and unblock the forbidden sites. Along with software dedicated to Web filtering, the best Internet security suite solutions offer parental controls, too. Also, find out what parental controls, if any, your Internet service provider offers.



• **Use monitoring software.** As a last resort, if you suspect your child is using the Internet inappropriately, consider installing monitoring software. These programs can record all your child's keystrokes, without their knowledge, and automatically e-mail that information to you.

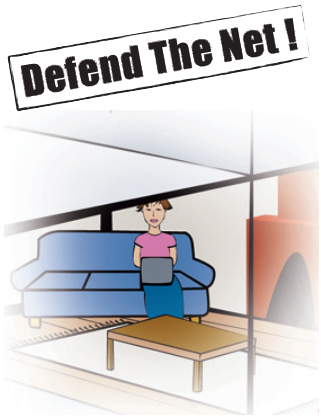
Surfing in peace

The Internet is by far the richest resource of news and information, and the most convenient tool for interpersonal communications, ever devised. Its rewards far outweigh its risks. But make no mistake: The risks are real, there are new ones every day, and they are increasingly more destructive.

Fortunately, you can protect your family from Internet threats easily and affordably. With the right security software, the proper precautions, and an awareness of your children's online activities, your family can surf the Web in peace.

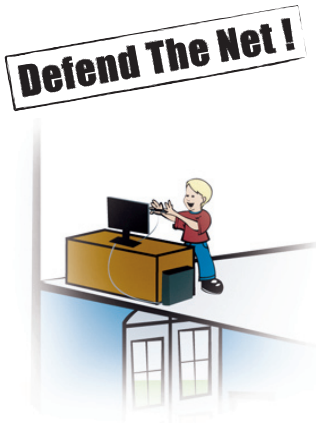
ZoneAlarm is an innovative Internet security company dedicated to protecting consumers worldwide (from the threats that abound on the 'Net-delete) with powerful technologies and easy-to-use solutions. For more information on our complete line of security software products, please visit www.zonealarm.com.

ZoneAlarm® by Check Point®



Internet Security Threats & Solutions: At a Glance

What's the Threat?	What Puts You at Risk?	What Can Happen?	How Do You Protect Yourself?
Spyware	Downloading files from file-sharing services; playing interactive games online; installing free software from unknown, untrusted sources	Spyware can make your computer unstable or unusable; enables others to record your keystrokes and steal your private data.	Install and regularly update antispyware software; perform frequent spyware scans; avoid sites and activities that can invite spyware
Viruses, worms, Trojan horses	Reading e-mail from unknown senders; opening unknown e-mail attachments	Your computer files can be destroyed; hackers can gain control over your computer; and viruses can quickly spread to other computers	Install and regularly update antivirus software; perform frequent antivirus scans; never open e-mail attachments you aren't expecting or e-mails from people you don't know
Hackers	Going on the Internet without firewall protection–particularly when using an always-on, broadband connection	Hackers can access your PC without your knowledge to steal your private data or use your computer for their own purposes	Install and regularly update PC firewall software on every PC you own. Make sure the firewall can protect you against unauthorized inbound and outbound communications
Identity thieves	Shopping, banking, or conducting other financial transactions at unsecure online sites or on unsecure connections	Thieves can steal your social security number, credit-card number, banking passwords, and more, costing you thousands of dollars	Make sure every online financial transaction is encrypted; avoid clicking on pop-up ads; don't allow third-party cookies to be downloaded onto your computer
Phishing scams	E-mails that appear to be from legitimate institutions, urging you to reply	Replying to a phishing scam can cause you to unknowingly provide criminals with your personal financial information	Never reply to e-mails asking for your passwords, account numbers, or other private information–no matter how legitimate they may appear to be
Sexual predators	Minors providing strangers with too much personal information in chat rooms, IM sessions, and elsewhere	Your child can be molested, harassed, taunted	Strongly warn children of the dangers online; monitor their Internet habits if necessary; and provide them with strong guidance about what is and isn't appropriate
Privacy intrusions	Clicking on pop-up ads; cookies that track your Web surfing habits;	Marketers and others can learn about your online habits, subjecting you to more pop-ups; identity theft is a possibility	Install and regularly update a PC firewall with privacy controls, such as pop-up ad blocking; never click on pop-ups; block third-party cookies
Spam	Having an active e-mail account	Your inbox fills up with useless, annoying, even pornographic junk e-mail messages	Use spam blocking tools in Internet security suites, e-mail applications, and other programs; find out what your Internet Service Provider offers for blocking spam
Instant messaging monitoring & spam	Instant messaging with friends, family, and colleagues	Outsiders can spy on your conversations, send spam, solicit children for sex, and more	Use a PC firewall or other software program offering full IM protection
Wireless network hackers	Using an unprotected wireless network at home or on the road	Hackers can log your keystrokes, steal your private data, direct you to fraudulent Web sites, and more	Encrypt your home wireless network; always use a PC firewall when connected to a public wireless network



Online Security Resources

The Web is full of helpful tips, tools, and information that can help you bolster your PC's security. Here are some sites to check out:

• **SafeKids.com** provides information on protecting children online. URL: www.safekids.com

• **GetNetWise** is a coalition sponsored by Internet industry corporations and public interest organizations, with resources on helping you and your family stay protected online. URL: http://www.getnetwise.org

• **ChatDanger** is designed to educate all users about chat room risks. URL: www.chatdanger.com

• **The Federal Emergency Management Agency** (FEMA)'s Online Safety guide features safety rules for kids. URL: http://www.fema.gov/kids/on_safety.htm

• **Internet Content Rating Association** offers a free, downloadable filter for blocking inappropriate Web content, plus tips and advice for kids and parents. URL: http://icra.org/

• **The New York Public Library** Web site features "A Safety Net For the Internet: A Parent's Guide." URL: http://nypl.org/legal/safety.cfm

• **The Federal Bureau of Investigation** has a page of Internet safety tips for kids. URL: http://www.fbi.gov/kids/k5th/safety2.htm

• **The National Cyber Security Alliance** provides a Web site, StaySafeOnline.org, with tips and advice for home users, students and teachers, and small businesses. URL: http://www.staysafeonline.info/

• **ProtectKids.com** is a good resource for recent statistics regarding Internet risks. URL: http://www.protectkids.com/dangers/stats/htm

• **PC Magazine** has published several useful articles about protecting yourself online. Here are two examples:

• A False Sense of Security," at http://www.pcmag.com/article2/0,1759,1755221,00.asp

• Head Off Spyware, Viruses and Malware," at http://www.pcmag.com/article2/0,1895,1819044,00.asp

• http://www.staysafeonline.org/