Safe Computing Tips

If you use your computer on the interent, then you need to be aware of computer viruses, worms, Trojans, and phishing. Why do you need to be concerned about these items?

1. Your user name and password, and your computer, can be used to send spam and viruses to other people, including your family and friends.
2. Your financial and personal information can be stolen.
3. Your identity can be stolen. It may take months of effort to clear yourself of false debts and restore your credit.

Suggestions to help you avoid viruses, worms, Trojans, and other computer malware.

1. **Install, use and update an anti-virus software**
   Choose a good anti-virus program. Suggestions are:
   Norton AntiVirus, included in Norton Internet Security
   McAfee VirusScan, included in McAfee Internet Security Suite
   TrendMicro PC-cillian includes antivirus, firewall, Spyware detection, anti-phishing

   Keep it up-to-date.

   Anti-virus programs can only protect you from what they know about. Since new viruses surface every day, it's very important for you to update your anti-virus program regularly.

   Use it!

   An unused anti-virus program is obviously useless. Use your anti-virus program to scan new files you just downloaded or to do routine scans. If you are not very knowledgeable about computers and viruses you may benefit from using the memory resident scanner. If, however, you know what you are doing, then you probably can live without it.

   Don't rely on it.

   Modern anti-virus programs detect malicious code quite reliably but it is very important to remember that NO anti-virus program is perfect. No anti-virus program on Earth can compensate for imprudence or unsafe software. No anti-virus program will ever detect all viruses all the time.

   Use it intelligently.

   Some anti-virus programs offer some questionable features and gadgets. You shouldn't use a feature just "because it's there". For example, AV scanner certification messages are essentially useless and only serve to advertise AV software.

   Unlike viruses, which infect files, Trojan horses are harmful standalone programs that pose as something else; they may masquerade as games, screen savers, or even utilities. But Trojans can be just as harmful as viruses—if not more so. Once a Trojan program is launched, it installs malicious code on your computer. From there, the Trojan may collect your passwords and mail them to the person who created the program or open a back door that lets hackers secretly access and control your system remotely.

Safe Computing Tips

2. **Install, use and update personal firewall software.** See programs suggested in item 1, above.

3. **Preserving your privacy.** Phishing is when you receive an email stating to be a bank, financial company, eBay, or Paypal. The email asks you to click on a link to their website, and verify your information. DON"T DO IT. If you think you need to check your information, then go to the web site directly in the browser address bar.

4. **Keep your operating system and programs patched (updated).**

5. **Consider using alternative web browser and email software.** Malware is typically written for Internet Explorer and Outlook/Outlook Express.

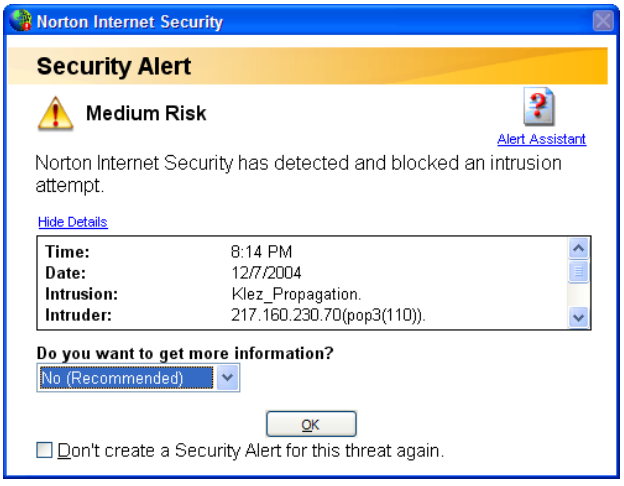
6. **Be cautious when reading email with attachments and downloading files.** Don't open files ending in **.exe**, **.com**, **.bat**, **.vbs** (Visual Basic Script), **.bin**, **.dot**, **.reg**, **.js**, **.xlm**, **.pif** and **.scr** (screensaver),

7. **NEVER, NEVER, NEVER, NEVER, NEVER, NEVER, NEVER OPEN ATTACHED .EXE FILES SENT TO YOU VIA E-MAIL!!!!!!**

8. **Other tips:**
    a. Use www.mailblocks.com to eliminate spam.
    b. Use bcc email distribution to avoid sending all email addresses to all recipients.
    c. Use disposable email addresses (such as at Yahoo or MSN)
    d. Use a credit card and bank account separate from your personal card and account, for Paypal.
    e. Use one-time-use credit card numbers from Citibank or MBNA.

9. **If you still get hit by a virus...** Symantec has a list of viruses and removal instructions. (http://securityresponse.symantec.com/avcenter/vinfodb.html)

The following graphic show that a virus was blocked from entering my computer. Use an antivirus program and a software firewall. Be Safe!



"1 in 10 Americans have been victims of ID theft in the last five years", Don't fall victim to the fastest rising crime in the county.

--> Are you unsure about your computer's safety?
--> Do you get popup ads when online?
--> Is your computer slow?

Answer yes to any of these and you probably have adware and spyware.

A study released by AOL and National Cyber Security Alliance found that over 80% of computers have adware and spyware.

Antivirus Software DOES NOT STOP adware and spyware! You need to run an adware and spyware program separately. Examples are Ad-aware (http://www.lavasoftusa.com/) and Spybot Search and Destroy (http://www.safer-networking.org/en/index.html).

Signs of being infected:

1. Your home page keeps changing
2. Slow running computer
3. Excessive popup advertisements
4. Toolbars appearing on your browser
5. Frequent system crashes.

If you, or someone using your PC, have downloaded Internet files such as music, games, screensavers, pictures or movies, then adware and Spyware programs have been added to your computer's hard drive without your direct knowledge. This "drive-by download" technique is rapidly growing - get your protection today.

Not protecting yourself against spyware/adware makes you easy prey for identity theft, computer corruption and pop-up ads. Spyware/adware can easily bypass your antivirus and firewall protection and install on your system without your knowledge. This is known as "stealth software". Spyware/adware programs are nearly impossible for most PC users to detect and remove.

New Computer? Six Steps to Safer Surfing

Washington Post, 12/18/04

(This is a summary of the article. See the pdf file to read the complete article.)

To see the e-mail I get every day from readers about security issues is to develop a deep discomfort with the state of computing today. Keeping a Windows PC safe can demand a high degree of vigilance.

And yet all these attacks by viruses, worms, spyware and browser hijackers could have been prevented with some initial effort. It's completely feasible to put a computer on the Internet -- even one running

Windows, the most attacked, least secure operating system around -- and never suffer a single successful attack.

Here's what to do to make that possible, starting -- as many people will this week -- when you take it out of the box and plug it in. Most of these steps apply only to Windows, but some pertain to Mac OS X (news - web sites) as well.

Step one is to barricade your Internet connection with a firewall. Without this, network worms such as Blaster can try to sneak onto your computer the instant it goes online, even if you don't run a single Internet program.

Step two is to download and install every security patch available. Don't do anything else online until the process concludes.

Step three is to activate and update the antivirus software on your computer. Most new PCs include only 90 days of updates, after which your protection will evaporate -- without a rap sheet on the latest viruses, your antivirus software can't identify them. Find out when your free coverage will end, then make a note in your calendar to renew your subscription before then.

Step four is to update three core Internet programs, since older versions can suffer from security flaws.

Step five is a big one: Download the free Mozilla Firefox Web browser (www.mozilla.org) and use that instead of Microsoft's Internet Explorer whenever possible. Firefox is not only simpler and more convenient than Internet Explorer, it's also much more secure -- since it's not hooked so tightly into Windows, it can't act as a transmission belt for viruses.

Step six is to use the most effective security mechanism ever invented, the human brain. In two words, be skeptical. Don't open unexpected e-mail attachments -- even if they come from a friend's e-mail address, since viruses scour infected PCs for e-mail addresses to impersonate. If you get an e-mail allegedly from your bank, ignore any links in it; log in by typing the bank's address into your browser yourself.

Most important, think twice about adding new, unknown software.

But there is no replacement, on any computer, for common-sense caution, the same thing that keeps people safe in the face of far worse dangers in the real world.

New IE Exploit Spoofs Web Sites

By Matthew Broersma, eWEEK
December 17, 2004

(This is a summary of the article. See the pdf file to read the complete article.)

Security researchers have uncovered a spoofing flaw in Internet Explorer that could allow a scammer to display a fake Web site with all of the attributes of a genuine, secure site.

The bug could allow a scammer to display a fake Web site with all the attributes of a genuine, secure site, including the URL and the icon indicating SSL security, according to researchers.

There is currently no patch for the bug. Users can protect themselves by turning off ActiveX or switching the security level for the "Internet" zone to "high," researchers said.
Microsoft has issued a "critical" update to fix a flaw in SP2's Windows Firewall. Click here for the full story. (http://www.eweek.com/article2/0,1759,1743123,00.asp)

"Once it is displaying the site, if you follow best practices and look for the padlock, et cetera, you still won't have a clue [that the site is spoofed]," Kristensen said. "It isn't really even spoofing—you are really visiting the site, it's just that another site is controlling what you see."

Unprotected PCs can be hijacked in minutes

USA Today Tue Nov 30, 7:13 AM ET

Excerpts from the article:

Surfing the Web has never been more risky. Simply connecting to the Internet - and doing nothing else - exposes your PC to non-stop, automated break-in attempts by intruders looking to take control of your machine surreptitiously.

While most break-in tries fail, an unprotected PC can get hijacked within minutes of accessing the Internet. Once hijacked, it is likely to get grouped with other compromised PCs to dispense spam, conduct denial-of-service attacks or carry out identity-theft scams.

Those are key findings of a test conducted by USA TODAY and Avantgarde, a San Francisco tech marketing and design firm. The experiment involved monitoring six "honeypot" computers for two weeks - set up to see what kind of malicious traffic they would attract. Once breached, the test computers were shut down before they could be used to attack other PCs.

The test did not measure Web attacks that require user participation, namely spyware, which gets spread by visiting contagious Web sites, or e-mail viruses, which proliferate via e-mail attachments. However, the results vividly illustrate how automated cyberattacks have come to saturate the Internet with malicious programs designed to take the quickest route to break into your PC: through security weaknesses in the PC operating system.

"It's a hostile environment out there," says tech security consultant Kevin Mitnick, who served five years in prison for breaking into corporate computer systems in the mid-1990s. "Attackers have become extremely indiscriminate."

Mitnick and Ryan Russell, an independent security researcher and author of *Hack Proofing Your Network*, were contracted by Avantgarde to set up and carry out the experiment.

Test results underscored the value of keeping up to date with security patches and using a firewall. Computer security experts say firewalls, which restrict online access to the guts of the PC operating system, represent a crucial first line of defense against cyberintruders. Yet, an estimated 67% of consumers do not use a firewall, according to the National Cyber Security Alliance.

The machines tested were types popular with home users and small businesses. They included: four Dell desktop PCs running different configurations of the Window XP operating system, an Apple Macintosh (news - web sites) and a Microtel Linspire, which uses the Linux (news - web sites) operating system.

Each PC was connected to the Internet via a broadband DSL connection and monitored for two weeks in September. Break-in attempts began immediately and continued at a constant and high level: an average of 341 per hour against the Windows XP (news - web sites) machine with no firewall or recent security patches, 339 per hour against the Apple Macintosh and 61 per hour against the Windows Small Business Server. Each was sold without an activated firewall. By contrast, there were fewer than four attacks per hour against the Windows XP updated with a basic firewall and recent patches (Service Pack 2), the Linspire with basic firewall and the Windows XP with ZoneAlarm firewall.

"The firewalls did their job," says Russell. "If you can't get to them, you can't attack them."
While attempted break-ins never ceased, successful compromises were limited to nine instances on the minimally protected Windows XP computer and a single break-in of the Windows Small Business Server. **There were no successful compromises of the Macintosh, the Linspire or the two Windows XPs using firewalls.** That pattern was not surprising, as Windows PCs make up 90% of the computers connected to the Internet, and the vast majority of automated attacks are designed to locate and exploit widely known Windows security weaknesses.

Intruders repeatedly compromised the Windows XP computer through the same two security holes used by the authors of the July 2003 MS Blaster worm and May's headline-grabbing Sasser worm, which overloaded computers in banks, hospitals and transportation systems worldwide.

To hijack the Windows Small Business Server, the attacker finagled his way into a function of the Windows operating system that allows file sharing between computers. He then uploaded a program that gave him full control.

On three occasions, intruders got as far as logging on to an Internet Relay Chat channel, signaling an intent to herd the compromised PC with other hijacked PCs to pursue illicit activities. IRC channels work like a private instant-messaging service. An intruder in control of such a channel can send instructions to some PCs to spread spam, to others to serve up scamming Web sites, and to others to hijack more PCs.

"Downloading and using other exploits, performing denial-of-service attacks, running spam-relay tools, running identity-theft tools are all very common activities of compromised machines," says Martin Roesch, chief technology officer at tech security firm Sourcefire.

The end game: illicit profits. Compromised PCs supply the computing power for cybercrooks to run increasingly diverse scams, including phishing schemes that lure victims into typing account information at counterfeit Web sites.

In the past month, the first phishing scam to plant a bogus Web link on a legitimate banking Web site surfaced. The scam was probably carried out with hijacked PCs to protect the perpetrator from detection. "It's the most sophisticated, and frightening, phishing scam we've seen," says Susan Larson, vice president of global content at SurfControl, an e-mail security firm.

Panic Over Spyware

PC Magazine, 12/20/04
By John C. Dvorak

(This is a summary of the article. See the pdf file to read the complete article.)

Dell support lines have been getting 70,000 calls a week regarding machine performance and anomalies. Dell has been referring the callers to Web sites discussing spyware. It's spyware causing the problems.

This subject is near and dear to me, since my laptop was infected via a hotel network connection recently. The culprit is the webrebates.exe Trojan horse. Like many of these pests, once it gets on your machine it starts installing loaders all over the place. These are essentially spyware spies. They all look to make sure that the spyware stays in place. If you manage to erase it one of the little drones will reinstall it. You cannot erase the drones and the spyware fast enough to prevent this simple process from continuing unless you use special software to ferret out all the drones first. Many of these pests also contaminate the Registry, and many of the drones are in subdirectories that cannot be seen using any normal process.

As an aside I should mention that I've always wondered why Microsoft Windows has weird deeply rooted directories that cannot be seen in Internet Explorer, DOS, or any tool. They are scattered all over the place. The nasty spyware drones often end up buried so deep that finding them requires lengthy deep searches by antispyware tools.

Now, if you think that the free antispyware programs are going to help with the nastiest of infections, you are kidding yourself. I've chatted with four spyware vendors over the past couple of weeks and they all agree that it's gotten so bad that the public is only partially aware of the problem. Few users know that their machines are infected.

There is now a firm belief that organized crime, including the Russian mafia, is behind much of this activity. The scene is no longer dominated by kids out for fun.

So what is the spyware used for? There appear to be four primary uses.

Market research. Yes, it's true. A lot of spyware is used just to track browsing and other online behavior for market-research companies. This was one of the two initial uses.

Employee and spousal monitoring. This is the second initial use for this stuff. Key loggers and other systems that are usually installed directly onto machines by the person or institution doing the spying. The FBI has been known to capture passwords using such software.

Spambots. The more recent use of spyware has been to create legions of spambots for spammers to rack up big numbers without taxing their own servers. There are probably millions of drone machines, sometimes called zombie PCs. At night they are brought to life to serve spam all over the world.

Identity and credit-card theft. This is the latest twist and the fastest-growing trend. Last week, a new combination scam somehow got through my spam-filtering mechanism and tried to install a Trojan horse loader onto my system through the preview window of Microsoft Outlook Express.

The notable thing about spyware is that because it isn't virulent like a virus and seldom spreads from your machine to another, it manages to stay out of the spotlight. The national media pay little attention to the problem, and many mainstream media tech writers are Mac users, so they don't get it. Who knows what will happen when the Mac community gets hit? They feel immune, and are for now. But when they get hit, there will be few resources to help them, since the antispyware community is busy with all the PC-related problems.

Since spyware has not spread quickly and tends to be installed via browsers one computer at a time, we are seeing slow—but relentless—growth. We can expect it to continue. I'm looking at all the spyware packages and I'll have a few to recommend in the months ahead. For now you'll probably need multiple systems to get rid of this stuff. This will be the number-one topic in the year 2005, guaranteed.

Reference material and details:

New Computer? Six Steps to Safer Surfing
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Six_steps_to_safer_surfing.pdf

New IE Exploit Spoofs Web Sites
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Spoofed_web_sites.pdf

Unprotected PCs can be hijacked in minutes
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/PCs_can_be_hijacked.pdf

Panic Over Spyware
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Panic_over_spyware.pdf

Computer Viruses
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Computer_viruses.pdf

Infection Protection
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Infection_Protection.pdf

Heading Off Spam
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Heading_Off_Spam.pdf

A Primer on Fighting Spyware
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/A_Primer_on_Fighting_Spyware.pdf

Anti-virus programs compared
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/anti-virus_pgms_compared.pdf

Netcraft toolbar blocks phishing
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Netcraft_toolbar_blocks_phishing.pdf

Bots March In
http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Bots_March_In.pdf