Email Concerns

Email is without a doubt the biggest source of security vulnerabilities on the Internet. All the qualities that make email so attractive to users—its speed, ease of use, inexpensiveness, and almost universal presence—also make it the perfect medium for spreading malicious software (malware). All the major virus, worm, and Trojan horse attacks have employed email to infiltrate networks worldwide. Therefore, email security is of the utmost importance to every user.

I recommend these two excellent webpages on email security that deal with all of the issues addressed in section and more.

Security Focus: "Securing Privacy: E-mail Issues"
http://www.securityfocus.com/infocus/1579

A Quick Guide to Email Security http://www.zzee.com/enh/email_security.html

Move Outlook and Outlook Express to the Restricted Zone[187]

One of the conveniences and one of the weaknesses of Outlook and Outlook Express are their intimate relationship with the Internet Explorer browser. If you use either Microsoft product for email, it is critical that you make sure they are moved to the **Restricted sites zone** of the Internet from their default location in the Internet Zone. Why? Because malware is often spread via email, so you need to be sure your security settings for your email reader are set very high.

By default, the Restricted sites zone is assigned the High security level. If you assign a site to the Restricted sites zone, it will be allowed to perform only minimal, very safe operations. However, I recommend you do not rely upon the zone slider being set to High; instead choose the **Custom** option for manual settings. It is not hard to do. Make sure your Restricted Zone settings are set to disable all Java, JavaScript, and ActiveX controls because these are the most frequent sources of security problems in email.

These are the generally accepted settings for the Restricted sites zone.

[187] Windows XP Service Pack 2 includes security upgrades to Outlook 2003 that are not covered here. Please see "Microsoft Outlook 2003 Security Tips" for more information. <http://security.fnal.gov/handouts/Outlook_2003_Handout.pdf > [PDF] (14 November 2006).

In Internet Explorer 6:

Tools | Internet Options | Security
Select: Restricted sites zone

- ActiveX Controls and plugins
  - Download signed ActiveX controls **[Disable]**
  - Download unsigned ActiveX controls **[Disable]**
  - Initialize and script ActiveX controls not marked as safe **[Disable]**
  - Run ActiveX controls and plug-ins **[Disable]**
  - Script ActiveX controls marked safe for scripting **[Disable]**
- Downloads
  - File Download **[Disable]**
  - Font Download **[Disable]**
- Microsoft VM
  - Java permissions **[Disable Java]**
- Miscellaneous
  - Access data sources across domains **[Disable]**
  - Allow META REFRESH **[Disable]**
  - Display mixed content **[Prompt]**
  - Don't prompt for client certificate selection… **[Disable]**
  - Drag and drop or copy and paste files **[Prompt or Disable]**
  - Installation of desktop items **[Disable]**
  - Launching programs and files in an IFRAME **[Disable]**
  - Navigate sub-frames across different domains **[Disable]**
  - Software channel permissions **[High Safety]**
  - Submit nonencrypted form data **[Prompt]**
  - Userdata persistence **[Disable]**
- Scripting
  - Active scripting **[Disable]**
  - Allow paste operations via script **[Disable]**
  - Scripting of Java applets **[Disable]**
- User Authentication: Prompt for user name and password

Once you have finished selecting the Restricted site zone settings, you are not finished yet. You must add your email reader (Outlook or Outlook Express) to the Restricted Zone.

Open Outlook Express or Outlook
Select: Tools | Options | Security
Select: Restricted Zone

For more details see:

About.com Email Help Center http://antivirus.about.com/library/bloutlook.htm

Don't Open Email Attachments

I can't say *never* open any email attachments because there are times when you trust the user and are expecting a document via email. However, do not open email or attachments from unknown or even questionable sources. If you don't know the person who is sending you an email, do not open the email or any file attached to it. Even if you do know the sender, be very careful about opening the email and attachment (people sometimes unwittingly spread malware). If the mail appears to be from someone you know, still be careful, especially if it has a suspicious subject line (e.g. "I love you" or "look at this!") or if it seems odd (e.g., it was sent in the middle of the night). It may not actually be from the person you know but may be using a "spoofed" or fake email address using your friend's identity. Also be especially wary if you receive multiple copies of the same message from any source because they are likely to be spam.

The best thing to do with suspicious email is to delete the entire message, including any attachment, and empty your email reader's trash. If you really must open a file from an unknown source, save it first and virus scan the file. However, you need to know there is still a risk because no virus scanning software can detect every piece of malware.

"Finally, remember that even friends and family may accidentally send you a virus or the e-mail may have been sent from their machines without their knowledge. Such was the case with the "I Love You" or "Love Bug" virus that spread to millions of people in 2001. When in doubt, delete!"[188]

Stop "Email Wiretapping" by Disabling JavaScript in Your Email

A malicious user could insert hidden JavaScript code into an HTML email message and send it to another person's email reader that has both JavaScript and HTML enabled. Then if that unsuspecting person forwards the email message to others, the JavaScript, using a web bug or hidden form, surreptitiously sends a copy of the forwarded email back to the original sender, who can retrieve and read the forwarded message. This is a great method for spammers to harvest email addresses. Turning off JavaScript in email offers some measure of protection for

[188] Awareness and Outreach Task Force, "Report to the National Cyber Security Task Force," 18 March 2004, < http://www.educause.edu/ir/library/pdf/SEC0403.pdf > [PDF], Top 10 Cyber Security Tips, p. 25, (1 February 2007).

you, but if you reply to or forward an email to a person with a JavaScript-enabled email program, that person is vulnerable.

JavaScript is disabled in **Microsoft Outlook** and **Outlook Express** by adding them to the Restricted Zone where the settings disable all Java, JavaScript, and ActiveX controls (do not just set the zone to "high"; you must choose the *Custom* option and do this manually). For detailed information on Email Wiretapping, see:

About's Email Wiretapping Article
http://antivirus.about.com/library/weekly/aa020501a.htm?once=true&

See What's Arriving in Your Email

Malicious hackers can easily disguise malicious file types sent via email using what are called "double extension" files. For example, you may think you've received a harmless graphic file in *.gif* or *.jpg* format when in fact the file is something else altogether—such as an executable or a visual basic script—and opening it can infect your computer. The reason you are being fooled is that Windows' default setting hides certain file types that are "known" to the operating system, so what you see is *prettypicture.gif* when the full file name is *prettypicture.gif.vbs*.

To see all file extensions, you need to make a simple change to Windows itself (*not* to your browser or email tool). To enable **show all files**:

Windows 2000

- Open **My Computer**.
- Select the **Tools** menu and click **Folder Options**.
- Select the **View** Tab.
- Under the **Hidden files and folders** heading select **Show hidden files and folders**.
- Uncheck the **Hide protected operating system files (recommended)** option.
- Click **Yes** to confirm.
- Click **OK**.

Windows XP

- Click **Start**.
- Open **My Computer**.
- Select the **Tools** menu and click **Folder Options**.
- Select the **View** Tab.

- Under the **Hidden files and folders** heading select **Show hidden files and folders**.
- Uncheck the **Hide protected operating system files (recommended)** option.
- Click **Yes** to confirm.
- Click **OK**.

HTML & Email: Two Things That Do Not Belong Together

One of the worst practices to gain widespread acceptance on the Internet is HTML email. Surprised? It sounds like a nice idea (I mean, don't HTML messages look a lot nicer than text?), but in reality it is the source of lots of problems. HTML was created for web browsers and webpages, and that's where it belongs. But somewhere along the way, someone got the "bright" idea that HTML would make pretty email messages, complete with graphics and scripts and all those things that go into webpages. Unfortunately, all the qualities that make HTML appealing and flexible also make it vulnerable and have created huge problems with email. Here are some (not all) of the major problems with HTML in email:

1. HTML often contains executable code, such as JavaScript, Java, or ActiveX, which can automatically do a number of things on your computer *without your doing anything* to activate it and without your knowledge or consent.

2. Email programs (such as Outlook and Netscape Messenger) often have bugs that have been exploited by email worms and viruses that include automatic execution of attachments, buffer overflows, etc. While the bugs have been systematically patched by their manufacturers, the fact is that many people do not install patches and new exploits come along all the time. HTML facilitates the spread of malicious software.

3. Macromedia Flash is a browser plug-in that "interprets" code, so it could be used to execute malicious code or initiate buffer overflows from a fancy HTML email message.

4. Web bugs (invisible clear images imbedded in HTML email) are used routinely both by advertisers and spammers to track who reads (that means OPENS) their email messages. When you VIEW the message, the web bug (image) is downloaded and a unique ID is sent back to the spammer/advertiser. Now he knows your email address is alive and well and ready to receive more spam! Some email readers prohibit the display of remote graphics in HTML email by default; these include but are not limited to Google's Gmail, Yahoo Mail, Mozilla Thunderbird, and Opera. Outlook 2003 with Windows XP SP2 adds anti-phishing functionality, displaying all junk email in plain text format and removing the ability to click on URLs in the junk email folder and on other suspicious messages.

A spreading threat involves something called image spam. **Image spam** uses HTML code to display the email message, so spam filters cannot detect the spam because there is no text. Some estimates place the amount of image spam at "15-25% of all spam sent in the first half of 2006."[189] Clever image spam emails appear to be plain text messages to the casual observer, but in fact the entire message is nothing but an image. While image spam at present appears to be mainly a nuisance, it has the potential to become a threat as malicious hackers figure out ways to exploit it.

What can you do to protect yourself and others. First, *never send HTML formatted email*. Period. It's easy to **select the format for your outgoing email:** [190]

Outlook Express 6:

Tools | Options | Send | Mail Sending Format
select Plain Text

Outlook (most versions):

Tools | Options | Mail Format | Message Format | Choose a format for outgoing mail | Send in this message format:
select Plain Text from pull-down menu

The next part is more complicated. Of the current versions of Microsoft's Outlook and Outlook Express, only Outlook 2003 and Outlook Express 6 give users the ability to disable HTML in messages *received*. This is a huge problem and one that a lot of users have solved either by switching to another email client, such as Eudora, or by installing a program, such as noHTML. As of now, if you use Outlook[191] or Netscape Messenger for email, you run the risk of falling victim to all the many perils of HTML email.

Outlook 2003: to disable HTML in messages you *receive*

Tools | Options | Preferences | Email Options

[189] Mike Chapple, "Battling Image Spam," Search Security.com, 15 August 2006, <http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1210679,00.html> (1 February 2007).

[190] If you run a different email package, please check its help files for information on how to disable HTML.

[191] There is a way to disable HTML in Outlook 2000 using Tools | Macros | Visual Basic Editor, but it's too complicated for my taste. However, for the less faint of heart, here's where you can get the instructions (*no guarantees on this one*...I've not tried it): "How to Disable HTML Email in Microsoft Outlook," Ostrosoft, <http://www.ostrosoft.com/vb/disable_html_email.asp> (14 November 2006).

check *Read all messages in plain text*

Outlook Express 6: to disable HTML in messages you *receive*

Tools | Options | Read

check *Read all messages in plain text*

Changing this option just changes how messages are displayed, not how they are stored. When a message appears containing HTML or RTF (Rich Text Format), an option will appear in the message allowing you to view the selected e-mail in HTML or RTF format. Also, even in plain-text mode, some URLs still show up as hyperlinks.

Disable the Preview Pane

There are some other things you can do to make your email more secure. One is to ***disable the Preview Pane***, which is a feature in Outlook, Outlook Express, and some other email readers that shows the contents of an email message before the user opens it. The Preview Pane actually opens the email, even if you don't intend to do so. Some of the scripts that malicious users send via email can activate automatically simply when the email message appears in the Preview Pane. Also, web bugs are activated when the message is previewed before opening it, so disabling the Preview Pane is a fairly good way to stop web bugs from acting as the little "homing beacons" they are. Of course, all this presupposes that you will NOT OPEN the message but will delete it unopened and then empty your "deleted messages" folder.

To disable the Preview Pane in:

Outlook Express:

View | Layout deselect Preview Pane (do NOT use the preview pane)

Outlook:

In the *Inbox*: View | deselect Preview Pane (it is a toggle between seeing and not seeing it)

Don't Become "Phish" Food

While "phishing" (or carding) is a scam that has been around for years, it has become an enormous problem recently. Phishing is the use of "spoofed" emails and fraudulent websites that appear to be authentic emails from and links to legitimate company websites designed to lure an unsuspecting user to a fake website where the user will be prompted to enter personal information. Phishing emails have tricked many hapless customers of reputable companies into providing personal data, such as user names, passwords, account numbers, social security numbers, etc. How does phishing succeed? These particular kinds of scam emails, which are criminal in nature, are very professional-looking and use the real companies' logos and, so it seems, web addresses to lure a user to a fraudulent website. Phishing attacks sometimes employ very convincing image spam to trick users. Even the link looks valid to the average user. Phishers are reportedly able to convince up to five percent of recipients to respond to them, and it doesn't take many successful phishing scams to pay big dividends for the criminals behind them.

One celebrated case of phishing involved Citibank. Here's how it worked. Let's say you are a Citibank customer and you get an email "from Citibank" (the email has the Citibank logo and looks as though it came from Citibank). One of the numerous fake Citibank emails says, "We encountered a billing error when attempting to renew your Citibank online banking services." The email then goes on to detail member information from the "Citibank" database and says, "Please take a moment to update your credit card information by clicking here and submitting your information." The email ends with the warning that if you do not take this action, "your service will be terminated!"

On the face of it, the "Citibank" link in the email may look completely legitimate:

https://www.citibank.com/signin/citifi/scripts/user_setup.jsp

However, such links are fake. If the user "mouses over" (moves the mouse over) the link, he will see this:

http://www.citibank.com:ac=8tcBs829uY3T23ue76Hg@FaStWay2StUIpqwrCh7L09j

Now this link might be legitimate, too, except that everything between the *http://* and the at sign (@) in this url is irrelevant, so the real url in this link is what follows the at sign. Not exactly a Citibank website!

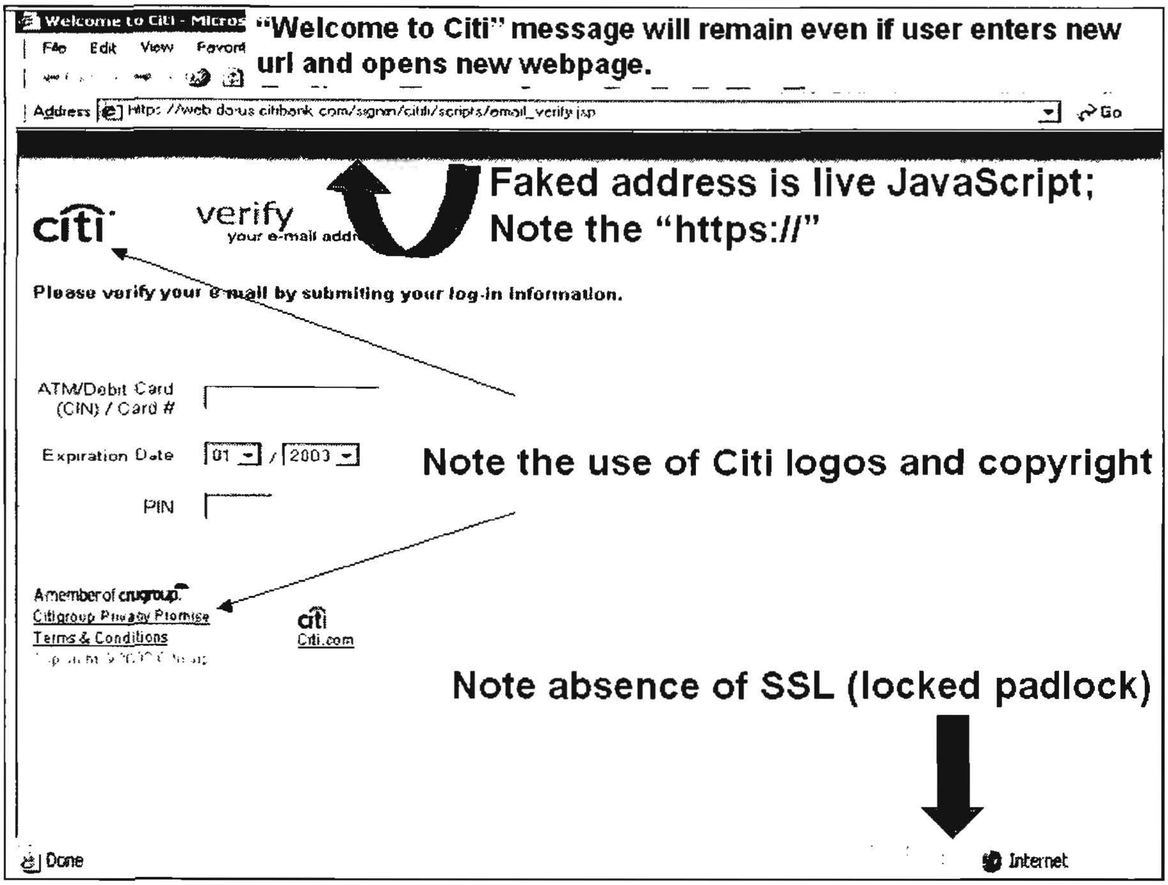
As consumers became more cautious and aware of these scams, new "bait" appeared in phishing scams that can fool even savvy Internet users. This attack uses a custom JavaScript to replace the Address or Location bar at the top of a web browser with a fake that is so good that it's almost undetectable. Here's how the attack works.

- Customer receives a forged but very legitimate-looking email from a bank or business with whom he may have a relationship (account, credit card, etc.).
- Email says customer must verify his email address and includes a link inside the email to a website.
- User clicks on the link in the email and the browser opens what appears to be the company's webpage but is in fact a fake website.
- The fraudulent site automatically detects the user's browser (the attack is not browser dependent) and runs custom JavaScript code that removes the real address bar and replaces it with a fake address bar at the top of the browser window. The copy is exact. It has the Address field, it displays a url that appears to be a secure link to the real company website (e.g. "https://"), and it has the *Go* button on the right-hand side. Unlike earlier, less sophisticated phishing attacks that create static (fake) Address bar images, this is a live piece of JavaScript code.
- Even if the user right-clicks on the webpage to View Source, the real source code is not shown; in order to see the real source code, the user must use the View | (Page) Source pulldown menu at the top of the browser to see the real HTML source code.
- The active JavaScript address bar could permit what is known as a "man in the middle" attack, i.e., every subsequent website the user visits after this one could send any information the user enters (passwords, credit card numbers, etc.) to the "phisherman" until the browser is closed.

In short, there are very few clues as to the fraudulent nature of this particularly dastardly phishing scam, but they are important ones:

- Even though the fake page shows the "https://" in the address bar, there is no corresponding Secure Sockets Layer (SSL) padlock at the bottom of the browser.
- If the user types a new url into the Address bar, the browser will continue to display the same fake "Welcome" message.
- The real url appears very briefly while the user is redirected to the fake site.

Take a look at this actual example of a fraudulent webpage used in a real phishing scam. You can see how it would be hard for the user to detect this is a fake.



"Welcome to Citi" message will remain even if user enters new url and opens new webpage.

Http://web do-us citibank com/signon/citi/scripts/email_verify jsp

Faked address is live JavaScript; Note the "https://"

Please verify your e-mail by submiting your log-in information.

ATM/Debit Card (CIN) / Card #

Expiration Date 01 / 2003

PIN

Note the use of Citi logos and copyright

Note absence of SSL (locked padlock)

There is a worrisome refinement of the traditional phishing attack that gained a lot of attention beginning in 2005. **Spear phishing** is exactly what it sounds like: precisely targeted phishing attacks that try to lure users to provide personal data by cleverly conceived social engineering strategies. Instead of the blanket approach of sending thousands (millions) of emails blindly, spear phishing carefully selects its audience and targets these users with very legitimate-sounding emails. For example, one spear phishing attack targeted students and faculty at the University of Kentucky. Spear phishing emails typically appear to be coming from a trusted source: your company's HR or IT department or your own little credit union. Also, a spear phishing attack may try to sound as if your security is at stake, e.g., you have been locked out of your account because of unsuccessful attempts to break into it, and in order to unlock your account you will need to reenter your personal information.

Fake spear phishing emails have even been used to educate people about the dangers of spear phishing. "In June 2004, more than 500 cadets at West Point received an email from Col. Robert Melville notifying them of a problem with their grade report and ordering them to click on a link to verify that the grades were correct. More than 80% of the students dutifully followed the instructions. But there is no Col. Robert Melville at West Point. Aaron Ferguson, a computer-security expert with the National Security Agency who teaches at West Point crafted the email. The gullible cadets received a 'gotcha' email, alerting them they could easily have downloaded spyware, 'Trojans' or other malicious programs and suggesting they be more careful in the future. Mr. Ferguson, who runs similar exercises each semester, said many cadets have been victimized by real online frauds."[192]

The problem with this approach is that it can undermine company trust. Who would ever trust another company email after being caught in a fake spear phishing attack? The fact remains, users must be extraordinarily vigilant and never provide personal information that is solicited by anyone without taking steps to verify the authenticity of that request. Sometimes a phone call is the best way to ensure that an email request from the HR person for your personal data really came from that department and not from a spear phisher.

How do you protect yourself from more and more sophisticated phishing scams?

- never, ever under any circumstances click on a link in an unsolicited email, especially one that asks you to click on the link to confirm or update personal or financial information.
- instead, type the address directly into the browser yourself and then check to see if that company has any security alerts about phishing scams.
- always make sure that the SSL is enabled before entering any personal or financial data; the browser will show a locked padlock: 🔒 or 🔒
- learn how to view and interpret the message source code of an email message; when in doubt about the true source, assume the worst.
- stay on top of the news about scams; frequent websites such as the one run by the Anti-Phishing Working Group.
- when in doubt, contact the source by telephone to make sure the request is legitimate.

For anyone concerned about phishing attacks (and that should be all of us), there are several free online tools to help you tell if a url in an email or on a webpage is legitimate (that is, is it what it says it is, or is it something entirely different?). These "url decrypters" are designed to reveal the real addresses of obfuscated urls. Nothing could be simpler to use: just copy the obfuscated url from an email or from a

[192] David Bank, "'Spear Phishing' Tests Educate People About Online Scams," *The Wall Street Journal Online*, 17 August 2005, <http://online.wsj.com/public/article/SB112424042313615131-z_8jLB2WkfcVtgdAWf6LRh733sq_20060817.html?mod=blogs> (14 November 2006).

webpage and paste it into the query box, hit return, and the hidden address will be revealed.

Sites to De-obfuscate URLs

URL Decrypter	http://www.cyber-junkie.com/tools/urldecrypter.shtml
Un-Obfuscating URLs	http://www.wilsonmar.com/1tcpaddr.htm

You must be very careful to avoid becoming "phish food" because the scams are increasingly sophisticated and hard to detect. Banks, lending institutions, insurance companies, and ***legitimate account holders*** of any kind (eBay, PayPal, Amazon, etc.) ***never send requests for account information via email***. If you are in doubt about any request for information via email, ***do not click on the link in the email***. Instead, open your browser, type the url of the company's home page into the browser's address bar and go to the site that way. Then you can log into your account and see if there is really a need for you to do anything. You can also use an online tool to de-obfuscate urls to determine the real address of any url. Phishing is a form of the con game discussed later.

Another potentially dangerous type of phishing scam involves fraudulent e-commerce websites that lure searchers to their sites, which present malware disguised as legitimate-looking images of a product supposedly for sale. The "image" is in fact a self-extracting zip (compressed) file that installs a Trojan horse on the user's computer, usually in order to steal personal and financial data. Be wary of any site that asks you to "click here to download images." This is an especially difficult scam to detect because many legitimate sites offer users the option to download image files (though usually not zipped files). The phishing sites purportedly are offering very inexpensive products, so if an offer looks too good to be true or if it looks in any way "phishy," it's best to avoid it.

A new type of attack gained prominence in 2006: "voice phishing" or **vishing**. Vishing is a type of phishing scam that uses VoIP (voice over Internet Protocol) phone numbers to trick users into providing their private information. Unlike traditional telephone numbers, it is relatively easy to get a VoIP number anonymously. "That makes it easier for scammers to carry out these vishing scams. In some ways, vishing may be even more dangerous than phishing scams, because consumers are used to entering private information into automated phone systems."[193]

Vishing indicates that as consumers wise up to scams such as phishing, bad people come up with creative new ways to separate you from your money (and sometimes your identity). One reason it's so easy to use a vishing scam is that some

[193] Issue #189, Scambusters.org, 26 July 2006, <http://www.scambusters.org/vishing.html> (12 December 2006).

companies, notably Skype, allow customers to pick both their area code and prefix, which means a call can appear to be coming from a very specific entity, such as your bank. The simple solution for customers is not to respond either to automatic emails (aka spam or phishing scams) or to automatic phone messages asking you to call a number. If you are in doubt about the legitimacy of any email or phone call, call your bank or credit card company at their main number and ask if there is a problem with your account. ***Good rule of thumb: Initiate, do not respond.***

How Not to Get Hooked by a "Phishing" Scam
http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm

The Anti-Phishing Working Group	http://www.antiphishing.org/
Phishtank (known and suspected phishing sites)	http://www.phishtank.com/

PayPal's Protect Yourself from Fraudulent Emails
https://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/SecuritySpoof-outside

Protect Yourself from "Pharming" Attacks

Not content with trying to lure victims to fraudulent websites using phony links in email messages, malicious users have devised an even more insidious trick to redirect users to fake websites. These scams have been dubbed **pharming**,[194] and the potential for the trouble they could cause is just becoming apparent. Basically, a pharming attack involves redirecting web users from a legitimate site by any number of dirty tricks. Usually the attacker exploits a browser vulnerability, such as what has been happening since late 2004 when the security company Secunia began identifying vulnerabilities in Internet Explorer, Opera, all the Mozilla-based browsers, and a number of other browsers that permit an attacker to inject content into a legitimate website, for example, by inserting the attacker's content into a popup at someone else's website. All these attacks are described as "spoofing" attacks, i.e., fooling users into believing they are at a legitimate website when in fact they are at a fake or spoofed site instead. Secunia provides details of these many vulnerabilities and demonstrations of whether your browser is vulnerable at its website.

Secunia's Advisories: Dialog Origin Vulnerability Test
http://secunia.com/multiple_browsers_dialog_origin_vulnerability_test/

It gets worse. In January 2005 a pharming attack successfully diverted all email and web traffic from the New York ISP Panix. According to a statement from Panix, "The

[194] This term may create confusion because there is already a use of the neologism pharming, i.e., "The production of pharmaceuticals from genetically altered plants or animals."

ownership of panix.com was moved to a company in Australia, the actual DNS records were moved to a company in the United Kingdom, and Panix.com's mail has been redirected to yet another company in Canada." How was this accomplished? According to Ed Ravin, systems administrator at Panix, "Our registrar, Dotster, told us that according to their system, the domain had not been transferred, even though the global registry was pointing at Melbourne IT. Something went wrong with the Internet registry system at the highest levels." This particular pharming attack involved a **domain hijack**, but it's not the latest type of possible pharming attack.

The newest browser vulnerability could enable even more sinister and harder to detect pharming attacks primarily because it is not a true vulnerability but rather simply an unintended side effect of a new browser feature designed to implement **International Domain Names (IDN)**.

This pharming attack does not involve a domain hijack. Rather, it is a spoofing attack that works by displaying fake addresses (urls) in the browser's address bar, the status bar, the hyperlinks, and even in the SSL Certificate. It is almost impossible to detect with the naked eye. The problem stems from the implementation of IDN, the standard that allows users to register domain names in different languages and different encodings. The flaw was first reported at ShmooCon, a hacking/computer security convention held in Washington, D.C., in January 2005. The Shmoo Group issued an advisory along with a demonstration of the attack using the domain for PayPal, in which they substituted an alternate Unicode character for the first "a." The address looks like the real PayPal url—http://www.paypal.com—but with a slightly smaller "a." With the implementation of IDN, there are now a huge number of ways to display domain names, many of which look very much like the original Latin character set.

The vulnerability affects IE7 (but not IE6 because IDN was not implemented before version 7). Firefox 1.0.6, Firefox 1.5 beta, Netscape 8.0.3.3, and Mozilla 1.7.11. The Firefox 1.5 release of November 2005 corrected the problem, so be sure you are using version 1.5 *or later* if you use Firefox. Previous versions of these browsers may also be affected. Mozilla released a self-installing patch that disables the International Domain Name (IDN) processing that makes the vulnerability possible.

Mozilla 1.7.12 http://www.mozilla.org/products/mozilla1.x/

Firefox http://www.mozilla.com/firefox/

"The State of Homograph Attacks," by Eric Johanson, The Shmoo Group, 31 Jan 2005 http://www.shmoo.com/idn/homograph.txt

Secunia's Multiple Browsers IDN Spoofing Test
http://secunia.com/multiple_browsers_idn_spoofing_test/

If you use a Mozilla-based browser or simply don't want to install the patch, there is a very simple workaround that negates the vulnerability:

- in the browser address bar, enter *about:config*
- scroll down to or search for the parameter *network.enableIDN*
- right-click on that parameter and select *Modify*
- change the value from *true* to *false*

Here are other suggestions for preventing this and other pharming/phishing attacks from being successful:

- never follow hyperlinks from HTML-formatted emails (in fact, don't accept HTML email in the first place); this is especially important in the case of emails from banks; and from companies such as Amazon, eBay, or PayPal; credit card companies, etc.
- do not click on hyperlinks from a website if you have any doubt about the site's integrity. You can always type the url into the address bar to ensure you go to the real website.

Go Offline to Read Your Email

You can go offline to read your email once you have downloaded it. You can tell Outlook Express to "Work Offline." Working offline in Outlook is more complicated, so I cannot recommend it. Also, if you are using a firewall program like Zone Alarm, it's easy to go offline. Just "lock" your Internet connection or block your email client's access to the Internet while you go through the junk email. There is no way the evil little web bugs can phone home to the mothership while your Internet connection is blocked or inactive. Then you can safely delete the messages (and *empty your deleted items folder*) before reconnecting. Of course, you will not be able to see any images or read any HTML emails that require access to a website, but you probably don't want to read these anyway because the ones that require access are likely spam or worse.

To work offline in Outlook Express:

in the Inbox: File | Work Offline

Try to Avoid Being Joe Jobbed

This may be hard to avoid. It's one of the oldest tricks around. Joe jobbing is an email spoof that sends out huge volumes of spam that appear to be from someone other than the actual sender. It got its name from its first known victim, Joe Doll, who offered free webpages to anyone who agreed to his rules of netiquette. In 1996 one of his free page users started sending newsgroup and email spam in violation of Joe's rules. When Joe terminated the user's free account, the spammer retaliated with forged messages that appeared to be from Joe Doll. The angry recipients of the spam that appeared to be from Joe in turn retaliated by attacking Doll's website, shutting it down for 10 days.

Because Joe jobbing is so easy to accomplish—sometimes nothing more than changing the *Reply-to* address is required—it's very hard to prevent. The best way to avoid being Joe jobbed is to follow the general rules for spam avoidance (and we all know how well these work). However, Joe jobbing tends to involve retaliation and is personal whereas spam is about as impersonal and universal as anything can get, so most people will be victims of the latter but not the former. Still, these are wise precautions for avoiding both the Joe job and spam.

- Don't unsubscribe from anything. Unsubscribing lets spammers know they have a valid email address.
- Don't open web-based emails as it also alerts spammers to a valid address.
- Don't open spam; simply opening spam may activate a script or web bug that alerts a spammer to a valid email address.
- Don't send and receive HTML email; it may contain code that alerts a spammer to a valid email address.
- Do not sign Guestbooks or, if you must, use a disposable email address, such as a Hotmail or Yahoo email account.
- Do not post your email address on a website. Email spiders can easily find and harvest your email address for spammers.
- Be very careful about signing up for anything free that requires your email address, especially newsletters.
- If you have ever posted to a newsgroup using your real email address, it's gone. Spammers have it. Get a new address.

For even more ways spammers gather email addresses and ways to avoid being harvested, see:

How Spammers Get Your Email Address
http://www.junk-mail.org.uk/articles/spam.html

First Spam, Now Spim

You thought spam was bad, but now there is a torrent of what has been dubbed “spim” or unwanted messages sent to instant messaging programs. According to a report from the technology market research company Radicati Group, spim tripled in 2004, growing to 1.2 billion spims sent, 70 percent of which are pornographic. While the number of spim messages is small compared to the estimated 35 billion spam messages in 2004, spim is growing at a rate of three times that of spam. Spim is also more intrusive than spam because spim messages pop up on a user’s computer screen when he is logged into his IM program, making them very hard to ignore.

While many IM users employ “buddy lists” to limit whose messages they can receive, spimmers have developed clever ways to get around this restriction by illegally “borrowing” identities or by persuading users to add them to their buddy list by posing as someone they are not. Experience shows that people are much more likely to click on spim messages than to open and/or respond to spam, in part because spim is not as well known and in part because it appears to be from a friend.

Celeste Biever, “Spam Being Rapidly Outpaced by 'Spim',” *NewScientist.com*, 26 March 2004,<http://www.newscientist.com/news/news.jsp?id=ns99994822> (1 February 2007).

Microsoft and Windows Concerns

The computer security company Symantec reported in 2006 that "home users now comprise 86 percent of all targeted attacks against computers,"[195] in large part because most home users do not take even the most rudimentary steps to secure their own computers. There is no such thing as a "secure" computer that is connected to the Internet. If you **never** connect your computer to the Internet—and by that I mean not for one minute ever—and never install any new software on your computer, you do not need to worry about computer security. Otherwise, you need to be concerned. I agree with Eric Vaughan of Tweakhound's assessment of the current state of computing:

> "1. There is no such thing as a secure OS (operating system), or web browser. If you want true security (read something like this somewhere at some time); *disconnect your network card, turn off/unplug your computer, take out the hard drive and smash it to bits, take computer to a construction site and ask the bulldozer operator to run over it.* [emphasis added]
>
> 2. In the real world, Windows operating systems are less secure than the newest versions of Linux (distro) and Mac OS X. We'll leave the argument over why that is and the advantages of one OS over another to internet forums/discussion boards.
>
> 3. A fully patched Windows XP and to a lesser degree Windows 2000 are the only non-server Microsoft OS's that are even remotely secure. If you care about security you shouldn't be running any other Microsoft OS's. If you have machines on your home network that run anything less than a fully patched XP, 2k, Linux (distro), OS X then the security of any machine on your network is lessened."[196]

To make matters worse, most home users are running Windows XP Home Edition. "Windows XP Home has too many major security flaws (e.g., in XP Home every default account has superuser privileges and cannot belong to any domain) to enable it to achieve even a baseline level of security."[197] However, there are specific

[195] Jay Wrolstad, "Hackers Targeting Home Computer Users," Newsfactor.com, 25 September 2006, <http://news.yahoo.com/s/nf/20060925/tc_nf/46488> (article no longer available).

[196] Eric Vaughan, "Securing Windows XP," Version 2 BETA, Tweakhound.com, 30 September 2005, <http://www.tweakhound.com/xp/security/page_1.htm> (14 November 2006).

[197] "Checklist for Securing Windows XP Systems," Lawrence Berkeley National Laboratory, <http://www.lbl.gov/cyber/systems/wxp-security-checklist.html> (14 November 2006).

steps you can take to improve your home computer security. It is important to keep in mind that every computer, like every person, is unique, which means I cannot cover every possible configuration that might occur. However, there are numerous excellent websites that discuss how to enhance security on a home computer and/or network, and I will point you to those sites.

Some of the best sites for home computer and network security for Windows' user are the following:

Tweakhound's Securing Windows XP
http://www.tweakhound.com/xp/security/page_1.htm

Fred Langa's 5 Essential Steps To PC Security
http://www.informationweek.com/shared/printableArticle.jhtml?articleID=177100010

NIST's Guidance for Securing Windows XP Home Edition
http://csrc.nist.gov/itsec/guidance_WinXP_Home.html

CERT's Home Network Security http://www.cert.org/tech_tips/home_networks.html

Gary Kessler's Protecting Home Computers and Networks
http://www.garykessler.net/library/protecting_home_systems.html

University of Cambridge's Securing Windows XP Home Edition for Stand Alone Use
http://www-tus.csx.cam.ac.uk/pc_support/WinXP/collegehome.html

Lawrence Berkeley Lab's Checklist for Securing Windows XP **PRO**
http://www.lbl.gov/ITSD/Security/systems/wxp-security-checklist.html

Windows XP Security Checklist
http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm

Tom-Cat.com's Secure Your Home Computer v.2.22
http://www.tom-cat.com/security.html

Download Operating System, Browser, & Other Software Updates Regularly

If you have a slow Internet connection, this is a painful process, but it is necessary. Many updates are in fact security patches in response to reported vulnerabilities. You should also be aware that the patches are not always explicitly described as fixing a security flaw. Updates are *not* the same thing as new version releases. New versions often (dare I say usually?) have new vulnerabilities, so the best advice is to wait until a new version has been around for a while before downloading it. Be sure to check Microsoft's Security page frequently for news, updates, and patches. Also, don't forget other software, such as Microsoft Office, which needs to be patched and updated separately.

If you are unlucky enough to be one of the many people who installed a Microsoft patch only to discover it caused problems with your computer, this article could come in handy.

Gregg Keizer, "How To Uninstall A Microsoft Patch," TechWeb News, 21 April 2006, http://www.techweb.com/wire/186500738 (31 October 2006).

Important: If you are using a router that offers additional ActiveX filtering, you will no longer be able to run Microsoft Updates with the filter enabled. You must disable (remove the check beside) any ActiveX filter on your router in order to update Microsoft products.

Microsoft Security Home Page	http://www.microsoft.com/security/
Microsoft Internet Explorer Security Updates	http://www.microsoft.com/windows/ie/downloads/default.asp
Microsoft Office Download Center	http://office.microsoft.com/downloads/
Microsoft Windows Update Page	http://update.microsoft.com/windowsupdate/

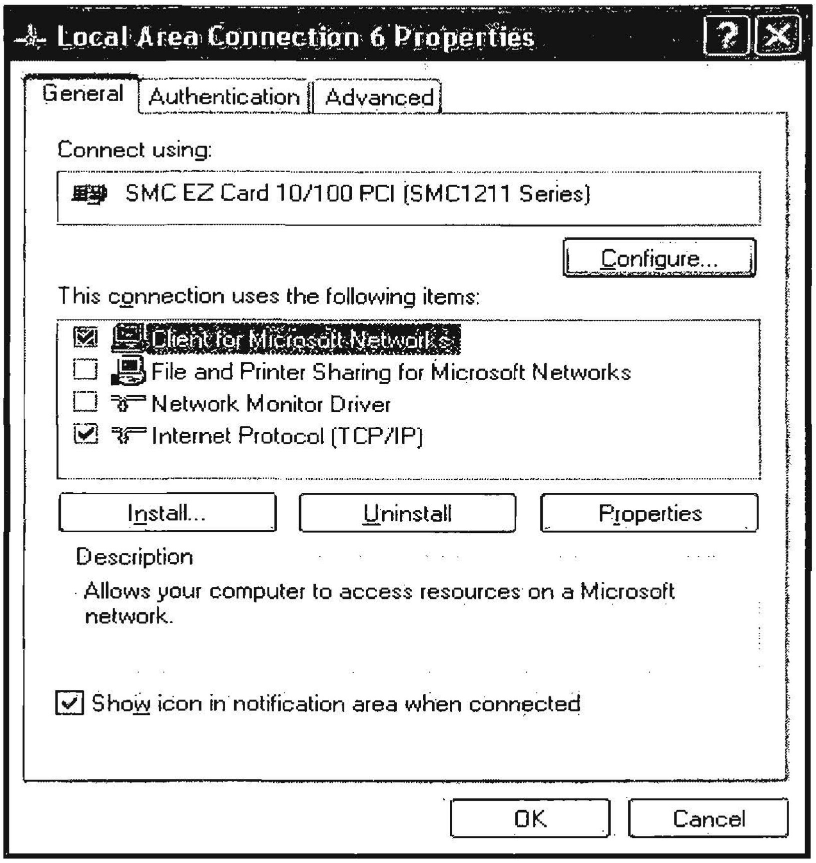
Turn Off File Sharing in Windows

You may or may not have file and print sharing enabled on your Windows computer. One of the changes in Windows XP Service Pack 2 (SP2) is that it includes the Windows Firewall, which is enabled by default in both the Home and Pro editions. And ***by default Windows Firewall blocks printer and file sharing***, which is the appropriate setting for most home users. Unless you need it, and you probably don't on your home computer, leave file and print sharing disabled.

However, if you turn off the Windows Firewall in order to use a better firewall, you may need to disable file and print sharing manually in order to thwart such cracking programs as "***ShareSniffer***,"[198] which is designed to find computers with file sharing enabled, access all the files on the hard drive, and perhaps modify or delete them. In any event, check your Windows' settings and make sure file and print sharing is disabled.

Windows XP. To disable file and print sharing in Windows XP:

1. Click the Start button in the lower left corner of the desktop.
2. Click Settings, then click Control Panel.
3. In the Control Panel, click Network Connections.
4. In the Network Connections window, right-click on the appropriate connection, then select Properties.
5. Uncheck the File and Printer Sharing for Microsoft Networks check box.
6. Click OK, then close the Control Panel window.



Connect using:
SMC EZ Card 10/100 PCI (SMC1211 Series)

This connection uses the following items:

☑ Client for Microsoft Networks
☐ File and Printer Sharing for Microsoft Networks
☐ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

Description
Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

[198] For more information on Sharesniffer, see Robyn Weisman, "New Hackerware Makes Everyone a Hacker," Newsfactor Network, 6 March 2001, <http://www.newsfactor.com/perl/story/7906.html> (14 November 2006).

Windows 2000. To disable file and print sharing in Windows 2000:

1. Click the Start button in the lower left corner of the desktop.
2. Click Settings, then click Control Panel.
3. In the Control Panel, click Network and Dial-up Connections.
4. In the Network and Dial-up Connections window, right-click on the appropriate connection, then select Properties.
5. In the Connection Properties window, click the Networking tab.
6. Uncheck the File and Printer Sharing for Microsoft Networks check box.
7. Click OK, then close the Control Panel window.

You may want to go one step further and unbind file and print sharing from TCP/IP, which (yet again) is the default setting for Windows. What does this mean? Simply, "the same capability that allows peer-to-peer networking and file sharing on your home/office LAN is available to anyone on the Internet!"[199] Instructions for unbinding print and file sharing from TCP/IP, which will still permit a local area network to share printers and files using a different protocol known as NetBEUI, are available at security expert Gary Kessler's website.

Securing Windows XP http://www.tweakhound.com/xp/security/page_1.htm

Protecting Home Computers and Networks
http://www.garykessler.net/library/protecting_home_systems.html

Disable Visual Basic Script in Windows

The infamous "Love Bug" worm exploited vulnerabilities in Windows Visual Basic Script via email. This is more than a browser problem because VBS (sometimes dubbed the "Virus Building System") is part of Windows, not the browser. There are several methods for thwarting potential VBS attacks. These sites all provide methods for preventing visual basic scripts from running automatically without your knowledge or consent. In addition, the first site offers detailed information about vulnerabilities associated with VBS.

How to Disable VBS	http://www.cvm.uiuc.edu/net/virus/outlook.html
Disable Windows Scripting Host	http://www.sophos.com/support/faqs/wsh.html
Remove Windows Scripting Host	http://www.f-secure.com/virus-info/u-vbs/

[199] Gary Kessler, "Protecting Home Computers and Networks," Gary Kessler.net, November 2002, <http://www.garykessler.net/library/protecting_home_systems.html> (14 November 2006).

Know What Your Computer is Loading (Check Your Start-Up Applications)

It seems that most programs today think they are important enough to start automatically each time you reboot your computer. That is, the default installation on most programs tends to add them to your Windows start-up list, so every time you start your computer, these programs are running whether you want them to or not. The problem with this is, at the very least, they are an unnecessary drain upon memory and other system resources and, at worst, some of these unknown programs may in fact be spyware or even viruses or Trojans that add any number of different entries to start-up.

Fortunately, most Windows operating systems (95/98/Me/XP) come with a handy System Configuration Utility called **MSCONFIG** that lets users identify start-up applications. The exception is Windows 2000, which does not come with msconfig. Before using this tool, I recommend you visit these excellent websites devoted to helping users demystify applications that run at start-up and explain which can be removed from start-up without danger. The sites also provide an exhaustive list of programs potentially residing in a computer's start-up list.

Greatis Start Up Application Database	http://www.greatis.com/regrun3appdatabase.htm
Pacman's Start-Up Applications	http://www.pacs-portal.co.uk/startup_index.htm
or	http://www.sysinfo.org/startupinfo.html

Know What Your Computer is Running

What exactly are those invisible programs running in the background on your computer using up system resources? Can you remove them safely or are they necessary? Are they spyware or Trojans undermining your privacy and security or maybe just useless junk clogging up the works? Or are they programs vital to keeping your operating system operating. It is very hard to tell because the names of so many of these programs are unrevealing, but there are several websites that help de-obfuscate these processes, tell you which ones you need, and recommend removal procedures when appropriate. However, it is very important to be careful about removing or disabling programs because many illegitimate programs have names that are almost—or in some cases are—identical to valid programs precisely to confuse users.

In order to see the processes running on your computer, the traditional method in Windows is to use Ctrl+Alt+Del to activate the Task Manager and view the Process

List, but in Windows 2000 and Windows XP, you can right-click on the task bar and select Task Manager.

Process ID maintains a large database of processes that might show up on the Process List. Process ID explains each process, its function, the associated program, and whether or not it is legitimate or malware. Process ID does not tell you how to remove unwanted or dangerous processes, but does refer you to free software designed to eliminate these types of threats.

The **Answers That Work** website provides a comprehensive and easily understandable database of most programs that any Windows user might see in his Task Manager. In addition to identifying the process, the site makes sensible recommendations about how to handle unnecessary or malicious processes. The site is selling a product, but you can handle most of the recommended removals by using the Start Up utility in MSCONFIG (above).

The Process Library will tell you exactly what the processes are, which ones must run, which ones can be safely disabled, and which ones are known threats. The Process Library is searchable by process name or alphabetically browsable. There is also a comprehensive DLL library. Both illicit processes and DLLs are identified as to the type of threat or problem (virus, Trojan, or spyware).

Process Library is also very good at explaining the nature of the problem and when a threat may be easily confused with a legitimate process or DLL. See, for example, the entry for *rundll32.exe*, which is a legitimate process on most Windows operating systems but may indicate a virus on Windows 2000 and XP. Do not, however, confuse *rundll.exe* with *rundll32.exe* or *rundll16.exe*...see, it is confusing. The problem with this site is that it, too, is selling something. When you do find a real threat or problem and click on the remove option, you are taken to a site selling a product to remove the process or DLL. However, Process Library is very good at identifying the many processes running on your computer.

Many of these problems can be avoided in the first place by keeping your virus scanning software up to date or, in the event you do get a virus, using that software to remove it. A very good site for help with removing a variety of types of malware—viruses, browser hijackers, exploits, Trojans, spyware—is PC Hell (motto: *You've Been Here Before But Now You're Just Visiting*). PC Hell doesn't try to sell you anything, just help save you from your current damnable situation, so to speak. So, once you have learned about your problem, it's worth a trip to PC Hell to see if there is a way out (sometimes, however, there is no exit).

Process ID	http://www.processid.com/
Answers That Work	http://www.answersthatwork.com/Tasklist_pages/tasklist.htm
Process Library	http://www.processlibrary.com/
PC Hell	http://www.pchell.com/

Shoot the Messenger!

With the release of Service Pack 2 for Windows XP, Microsoft finally shut one of the many wide open, unlocked "doors" in one of its operating systems by disabling Windows Messenger Service as the default setting. Unfortunately, Windows Messenger Service remains a problem for other operating systems. First, it is important to understand that ***Windows Messenger Service is something entirely different from instant messaging services and turning it off will not affect IM in any way***. Messenger is primarily used by network administrators to send administrative alerts to network users or, for example, to let a user know when a print job on a network printer is complete. However, most home users are not networked and never need or want Messenger. The problem is that Messenger comes enabled by default on most Windows operating systems and is, in fact, automatically launched whenever a user boots his computer. This may not sound too bad, except that the ever-enterprising spammers and malicious hackers of the world found a way to exploit the darned thing. The spammers found they could flood users with pop-up messages using Messenger and, worse, malicious hackers found a way to use a buffer overflow in Messenger to install and run malicious code on a victim's computer.

If you use a Windows operating system other than Windows XP/SP2 or Vista, I recommend you turn off Messenger Service—that is, if you can. Users of Windows 2000 systems can disable Windows Messenger Service. However, ***Windows Messenger Service cannot be disabled on Windows 98 or ME***. For Windows 2000 users, it is easy to disable Windows Messenger and, if needed, turn it back on by reversing these steps:

Windows 2000

Click Start | Settings | Control Panel | Administrative Tools | Services

Scroll down and highlight "Messenger"

Right-click the highlighted line and choose Properties.

Click the STOP button.

Select Disable or Manual in the Startup Type scroll bar

Click OK

User Profiles and the RunAs Command in Windows XP

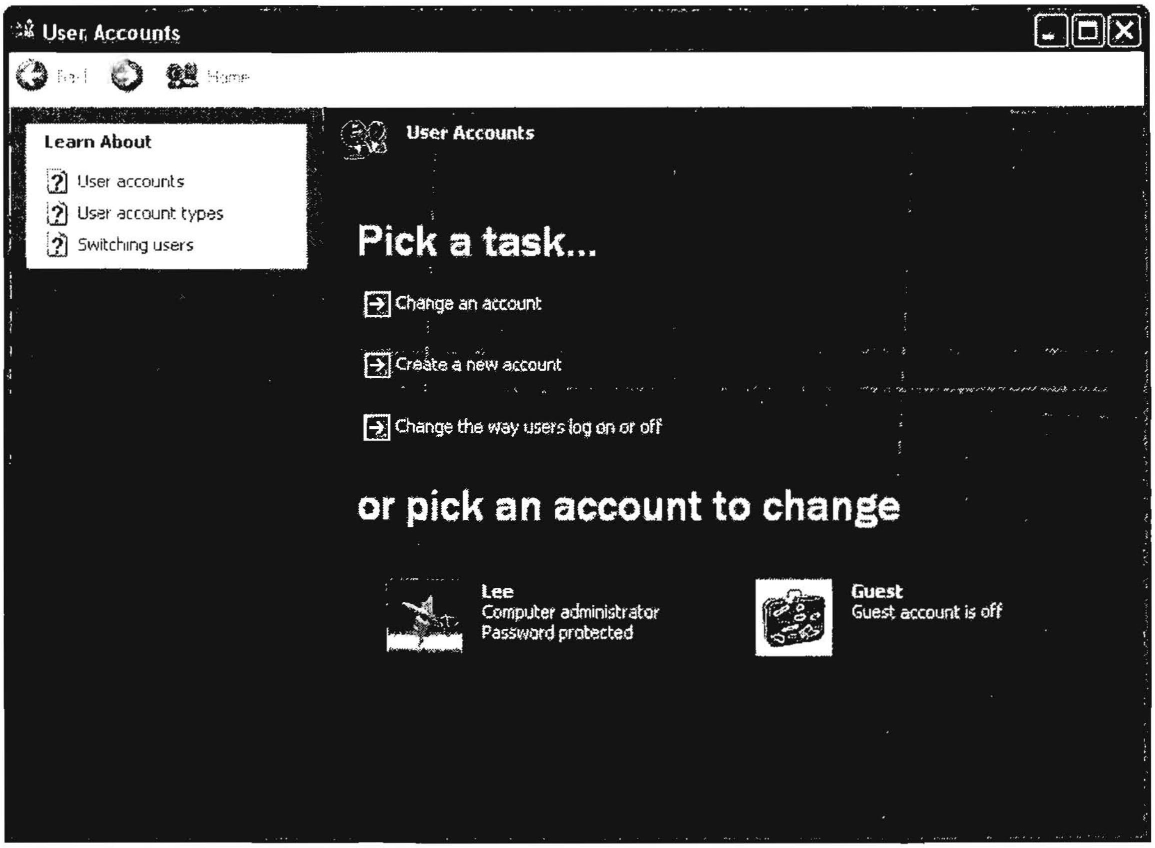
One of the best features of Windows XP, even in the Home Edition, is user profile administration and the *RunAs* command. While these options existed in Windows 2000/NT, Windows XP was the first Microsoft operating system to make these very important computer management and security features easily accessible and configurable for the home user. Although Windows XP Home Edition offers limited user and profile management when compared to the Professional Edition, it does introduce the concept of the Administrator versus the user as part of its **user accounts**. You should set up different types of accounts on your computer(s) running Windows XP Home Edition. Here's why and how.

Windows XP automatically creates certain built-in groups when it is installed. In Windows XP Home Edition, you belong to one of two broad types of "Groups": either Administrator or User. Belonging to a group gives a user rights and abilities to perform various tasks on the computer. Unfortunately, in Windows XP Home Edition ***by default, all user accounts have administrative privileges and no password***. This is a potentially serious security vulnerability that should be remedied right away. If you always use your computer as the Administrator, it means that, if you encounter a virus, a Trojan horse, or a worm while you are logged on as Administrator, your entire system could be compromised because the Administrator has full control over every aspect of the computer. When you are logged on as Administrator, ***every program you run has unlimited access to your computer***. If malware finds its way to one of those programs, it also gains unlimited access. However, if you create user accounts and normally log in as a user and not as the Administrator, any malware you encounter will be limited in the amount and kind of damage it can do to your computer.

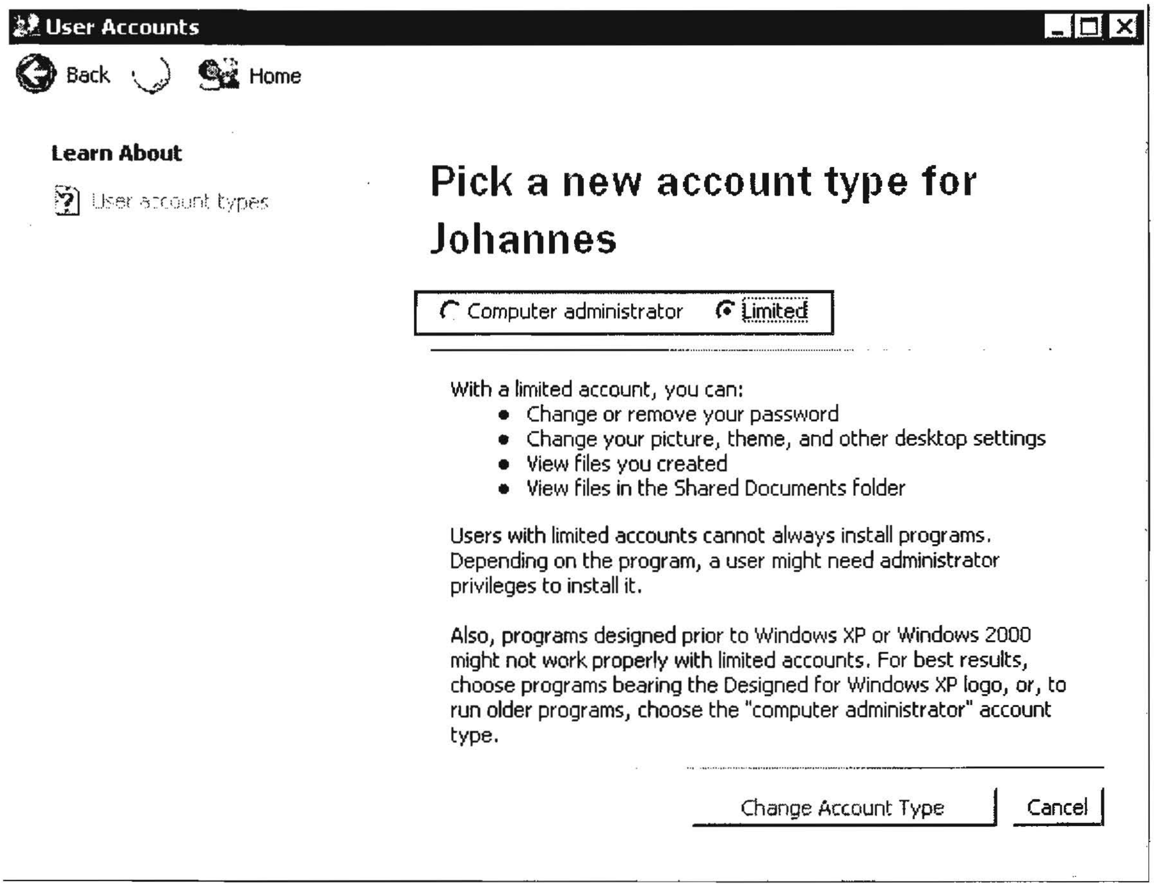
Here is how to set up user accounts in Windows XP Home Edition.[200]

[200] Windows XP Professional has additional user categories, including Power User, that are absent from the Home Edition. If you have Windows XP Pro at home, you have more options for how to administer your computers and your network.

- Logon as Administrator
- Start | Settings | Control Panel | User Accounts



From here, it is a simple matter to set up and change user accounts and account types. Create a "Computer administrator" account for yourself with a strong password. Then create a new account for yourself and each user of the computer as a Limited user. Make sure each Limited user account also is password protected. Remember, user names are not case sensitive but passwords are.



Pick a new account type for Johannes

○ Computer administrator ● Limited

With a limited account, you can:

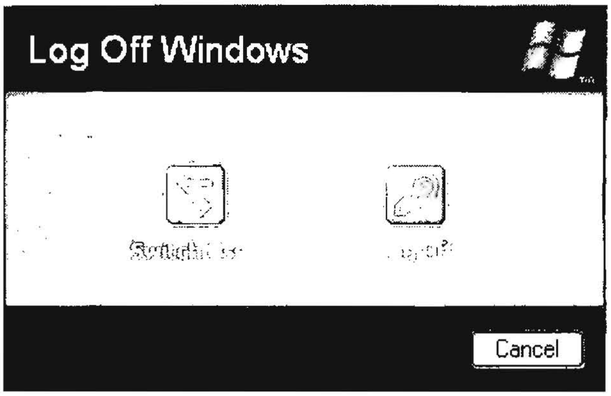
- Change or remove your password
- Change your picture, theme, and other desktop settings
- View files you created
- View files in the Shared Documents folder

Users with limited accounts cannot always install programs. Depending on the program, a user might need administrator privileges to install it.

Also, programs designed prior to Windows XP or Windows 2000 might not work properly with limited accounts. For best results, choose programs bearing the Designed for Windows XP logo, or, to run older programs, choose the "computer administrator" account type.

As you can see, Limited users are just that: strictly limited to what they can and cannot do on a computer. For the most part, logging in as a limited user should cause no problems in using applications on the computer. Email, web browsing, and instant messaging do not require administrative privileges, and are common avenues for malicious code to attack end users' systems. However, certain actions—such things as installing software, creating new network connections, or even running certain programs—require you to access them as the Administrator. There are two simple ways to accomplish this. First, you can always switch from Limited user to Administrator:

- Start | Log Off
- at this point, a new screen will appear; select **Switch User** and logon as the Administrator.

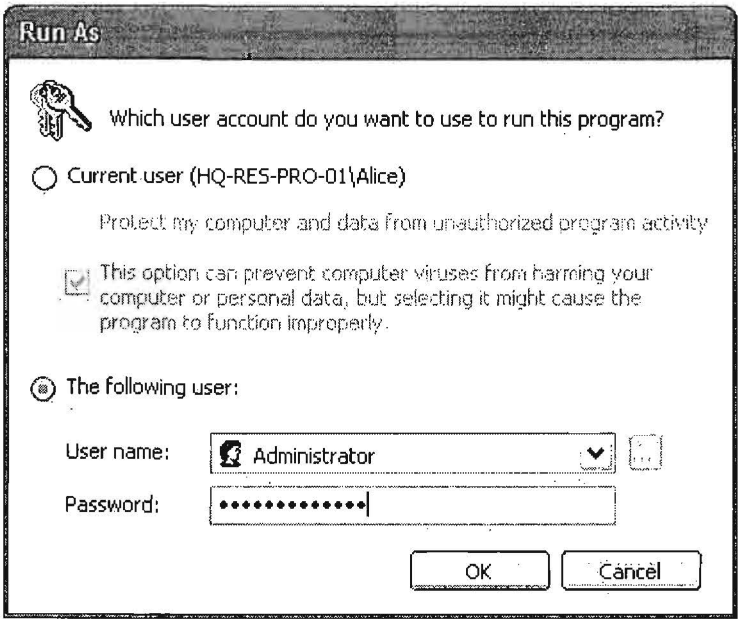


Fast User Switching should be enabled on Windows XP Home Edition by default, but just in case it isn't here is how to enable it:

- To Enable or Disable Fast User Switching:

  1. Start | Settings | Control Panel | User Accounts
  2. Pick a Task | **Change the way users log on or off**
  3. On the **Select logon and logoff options** page, check **Use the Welcome screen** and **Use Fast User Switching**

The second and, to my mind, much easier way to "be" the Administrator temporarily is to use the **RunAs** command. To sign on as Administrator using the RunAs command, simply right-click on a shortcut and select RunAs. When you right-click on a shortcut or application, you will see this dialog box, which gives you the option to run this specific program as the Administrator. As long as you know the user name and password, you can sign on as the Administrator or as any other user. This is an invaluable tool because a number of programs simply will not run for Limited Users. Keep in mind, however, that the RunAs command gives any Limited User the power of the administrator, so only permit a trusted user to use the RunAs command. That means if you don't trust your teenager to use RunAs responsibly, do not give him or her the administrator password. In this case, Windows XP Professional is a better choice because it gives you more user options.



Run As

Which user account do you want to use to run this program?

○ Current user (HQ-RES-PRO-01\Alice)

Protect my computer and data from unauthorized program activity

☑ This option can prevent computer viruses from harming your computer or personal data, but selecting it might cause the program to function improperly.

● The following user:

User name: Administrator

Password: ••••••••••••••

There is one more user account type that needs attention in Windows XP Home Edition: the **Guest account**. Guest accounts have been notorious gateways for malicious hackers to break into computers. Unfortunately, in the Home Edition you cannot (or, rather, *should* not) disable the Guest account ("disabling" the account from the Control Panel simply removes the Guest account from the Fast User Switching system). According to the Microsoft website, "You can use the **User Accounts** tool in Control Panel to turn off the Guest account. When you turn off the Guest account, you remove the Guest account from the **Fast User Switching** welcome screen. However, the Guest account is not disabled. We do not recommend that you disable the Guest account. If you disable the Guest account, you may not be able to access network resources. Additionally, you cannot access resources on a local computer from another computer on the network."[201] Okay, so do not try to disable the Guest account in Windows XP Home Edition. What can you do to minimize the risk posed by the Guest account? At this time, the best work-around is to ***assign the Guest account a very strong password***.

Sounds simple enough, doesn't it? Yet for some reason I really cannot comprehend, Microsoft failed to include an option to add a password to the Guest account in Windows XP Home Edition. However, all is not lost; you can still create a password for the Guest account very simply.

[201] "Description of the Guest User Account in Windows XP," Microsoft.com, <http://support.microsoft.com/default.aspx?scid=kb;en-us;300489> (14 November 2006).

- Logon as Administrator.
- Open a Command Prompt (Start | Settings | Accessories | Command Prompt).
- Type **net user guest *password*** (replace the word *password* with your new Guest password and make sure it is a strong password because no Guest password is better than a weak one.)

In summary, as Aaron Margosis advocates in his excellent "non-admin" blog, "do your everyday computing as a Limited user and log on as Administrator only when it is absolutely necessary, such as when installing new software or hardware, or changing security settings." Words to live by. For more detailed information about administering accounts, securing Windows XP Home Edition, and using RunAs on Windows XP Home Edition, refer to these links:

5 Steps to Secure Windows XP Home
http://netsecurity.about.com/cs/windowsxp/a/aa042204_2.htm

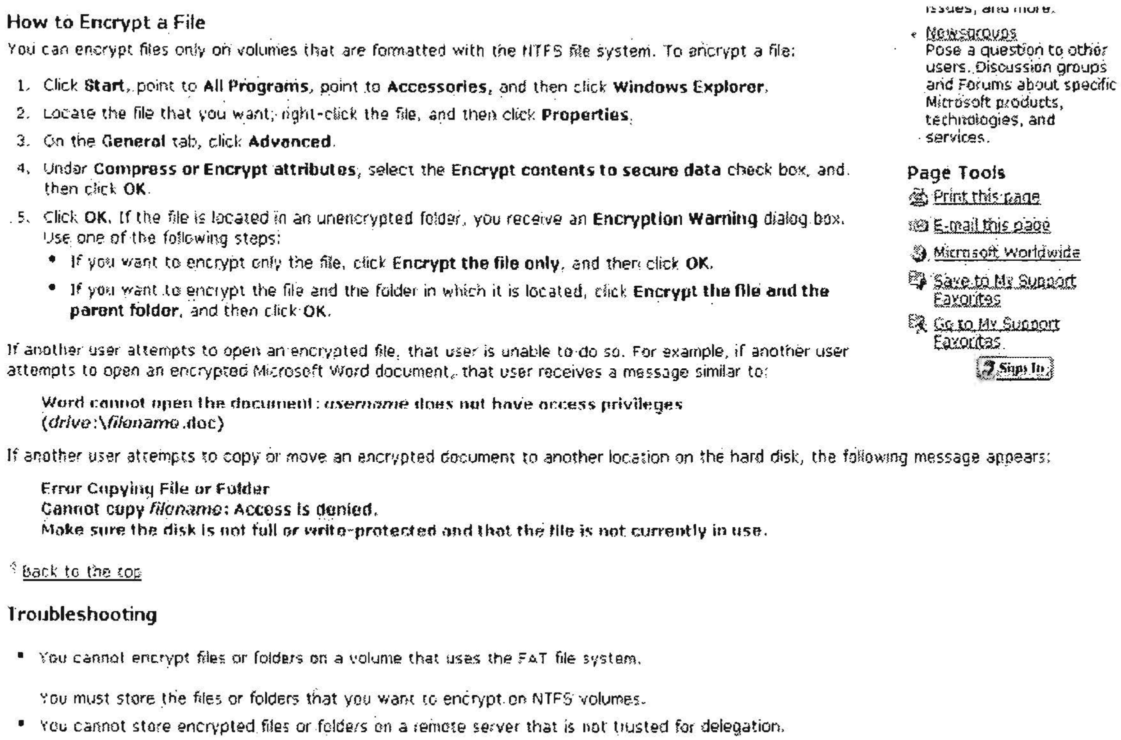
Non-Admin Blog, Aaron Margosis' Weblog
http://blogs.msdn.com/aaron_margosis/archive/2005/04/18/TableOfContents.aspx

"RunAs" basic (and intermediate) topics, Aaron Margosis' Weblog
http://blogs.msdn.com/aaron_margosis/archive/2004/06/23/163229.aspx

Encrypt Files in Windows

One of the basic privacy and security functions some versions of Windows offer is easy to use and provides a better degree of protection for files on your personal computer. However, not all Windows versions have this feature. ***The Windows operating systems that offer Microsoft's Encrypting File System (EFS) are XP Professional (another reason to go with Pro over the Home edition) and Windows 2000, beginning with Service Pack 2.*** Since most readers are probably using Windows XP, I will only discuss this operating system.

Microsoft provides clear instructions on how to encrypt a file in Windows XP Professional; keep in mind you can either encrypt a single file or a file and its parent folder.



How to Encrypt a File

You can encrypt files only on volumes that are formatted with the NTFS file system. To encrypt a file:

1. Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Windows Explorer**.
2. Locate the file that you want, right-click the file, and then click **Properties**.
3. On the **General** tab, click **Advanced**.
4. Under **Compress or Encrypt attributes**, select the **Encrypt contents to secure data** check box, and then click **OK**.
5. Click **OK**. If the file is located in an unencrypted folder, you receive an **Encryption Warning** dialog box. Use one of the following steps:
   - If you want to encrypt only the file, click **Encrypt the file only**, and then click **OK**.
   - If you want to encrypt the file and the folder in which it is located, click **Encrypt the file and the parent folder**, and then click **OK**.

If another user attempts to open an encrypted file, that user is unable to do so. For example, if another user attempts to open an encrypted Microsoft Word document, that user receives a message similar to:

> **Word cannot open the document: *username* does not have access privileges (*drive*:\*filename*.doc)**

If another user attempts to copy or move an encrypted document to another location on the hard disk, the following message appears:

> **Error Copying File or Folder**
> **Cannot copy *filename*: Access is denied.**
> **Make sure the disk is not full or write-protected and that the file is not currently in use.**

Back to the top

Troubleshooting

- You cannot encrypt files or folders on a volume that uses the FAT file system.

  You must store the files or folders that you want to encrypt on NTFS volumes.
- You cannot store encrypted files or folders on a remote server that is not trusted for delegation.

issues, and more.

- Newsgroups
  Pose a question to other users. Discussion groups and Forums about specific Microsoft products, technologies, and services.

Notice that ***only the user who encrypted the file or folder can open, copy, or move that file or folder***. If you keep information such as your passwords, financial information, etc., on your computer, especially if that computer is connected to the Internet, you should encrypt those files. In addition to adding a password to a sensitive Microsoft Office files, it is also a very good idea to encrypt those files as well.

How to Encrypt a File in Windows XP	http://support.microsoft.com/kb/307877
How to Encrypt a Folder in Windows XP	http://support.microsoft.com/kb/308989

For those who really want the nitty gritty on the EFS:

Windows XP Professional Resource Kit, Using Encrypting File System
http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/c18621675.mspx#EVD

Do Not Save Encrypted Pages to Disk

Internet Explorer uses caching to save website information as you browse in order to allow faster access to pages you frequently visit. The actual copies of webpages are stored in the Temporary Internet Files folder on your hard drive. Normally, this process is a benefit to users, but there is one circumstance in which you do not want pages saved. If encrypted webpages are cached, the copies saved to your hard drive are not encrypted and can be read by someone who might gain access to your computer using malicious software such as a Trojan horse or virus (or even someone with physical access to your computer).

To prevent this from happening, select:

Tools | Internet Options | Advanced | Security

- Check box next to "Do Not Save Encrypted Pages to Disk"

Next, you need to erase any encrypted pages that might have already been saved to disk.

Tools | Internet Options | General | Temporary Internet Files | Delete Files

In pop-up message that says "Delete all offline content," click OK

Handle Microsoft Files Safely

It can be risky to open certain Microsoft file types, especially those you may encounter on the Internet or in email, because of the potential for infection via what are known as macro viruses. **Macro viruses** exploit an application such as Word or Excel (which use little programs called macros) to infect a document and then spread the infection to other computers and networks. One of the dangers with macro viruses is that they do not infect programs, so you do not have to run an executable file to become infected. All you need to do is to open an infected Word, Excel, Access, or PowerPoint file to activate the virus.

However, there are some simple precautions you should take to avoid the risk of infection. After all, the awful Melissa virus of 1999 was a Word 97 and Word 2000 macro virus, and it spread like crazy around the world very quickly as an email attachment. There was another major outbreak of Word macro viruses in 2006, so the problem is still very much with us. As more search engines make it possible to search for non-HTML file formats, including all Microsoft file types, it is vital to take steps to protect yourself and your employer from potentially damaging viruses that could lurk in these types of files.

There are several ways to handle the problem of macro viruses and prevent both infection and spread of these nuisances:

- ➢ One of the safest and easiest ways is to use **Google** or **Yahoo** to locate the web page with the link to the file you wish to view, then select *view as html* or *view as text*. These options will permit you to see the file (whether it is a .doc, .xls, .ppt, .ps, etc.) as an HTML file or a text file (in the case of Postscript files in Google) with no fear of viruses.

- However, this solution will not work in every situation. There is an alternative available to users with access to Keyview Pro viewers. These viewers should be able to handle most file types you will encounter and handle them safely because the viewers do not run the underlying program and thus cannot execute a virus. The viewers also permit printing and some other functions. Documents should be saved to your computer's desktop; then right-click on the document to select the "View with" option. DO NOT DOUBLECLICK to open or you will execute the underlying program and possibly a virus as well. Here are the available viewers and the types of files they handle (this is not a complete list):

  Keyview Pro
  Microsoft Word
  Microsoft Excel
  Microsoft PowerPoint
  Applix Words
  Corel WordPerfect
  Corel Presentations
  Corel Quattro Pro
  Lotus Freelance Graphics
  Lotus 1-2-3
  Lotus Word Pro
  XyWrite for Windows
  Enhanced Metafile (EMF) (KeyView Pro 32-bit only)

  Adobe Acrobat
  PDF
  FrameMaker

  GSView/Ghostscript (GSView is a Windows GUI for Ghostscript)
  Postscript
  PDF

- Did you know that Microsoft offers free viewers for Word documents, Excel spreadsheets and other applications as well, including PowerPoint and Access files? This freeware lets you open, view, and print all Microsoft Office files without concerns about macro viruses because the viewers cannot run macros. The free viewers are built to automatically configure themselves for use with both Mozilla and Internet Explorer. They are available at:

All Microsoft Office Viewers	http://www.microsoft.com/office/000/viewers.asp

- As an additional precaution, make sure all your Microsoft applications have macros security settings at high. For example, in Word 2000:

1. open Tools | Macro | Security

2. select Security Level High

3. make sure there are no Trusted Sources

Doing this will ensure that no macros can run on your computer in Word because Word will not execute any macros at all with these settings.

- Configure your virus scanning software to perform an automatic virus scan of ALL downloaded files. Ensure that your virus scanning software ***scans all downloaded files***, not just executables.

An excellent guide to home network security is available on line from the CERT Coordination Center.

Home Network Security from the CERT Coordination Center
http://www.cert.org/tech_tips/home_networks.html

"Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore."

Handle with Care: More Privacy and Security Concerns

Use Anti-Virus Software and Keep It Up To Date

I expect most readers have anti-virus software on their computers, but having it and using it properly are not the same thing. Make sure you configure the software to maximize protection of your computer, especially against email-borne malware, run a full system scan at least once a week, and keep your virus definitions up to date. Most anti-virus software now offers automatic updates and scans, which can relieve users of some of the burden of remembering these tasks. There are new viruses—not to mention Trojan horses and other nasty invaders—unleashed via the Internet every day. The Kaspersky Lab's **VirusList** encyclopedia contains more than 30,000 entries. No anti-virus software is a guarantee against infection, but not using and updating it is akin to leaving your car door unlocked and the keys in the ignition.

There are several good free anti-virus packages, and AOL began offering "free" virus scanning software from Kaspersky during 2006. However, I would be careful about the AOL package, which is only free for 30 days; after that, there is a $50 per year subscription. I recommend reading Fred Langa's article[202] about the AOL offer before making a decision.

About's Free Antivirus Software Reviews
http://antivirus.about.com/od/freeantivirussoftware/Free_Antivirus_Software.htm

VirusList Virus Encyclopedia http://www.viruslist.com/en/viruses/encyclopedia

"Law #8: An out of date virus scanner is only marginally better than no virus scanner at all."

[202] Fred Langa, "Should you use AOL's free antivirus?" Windows Secrets and Langalist, 7 December 2006, <http://windowssecrets.com/comp/061207/#langa0> (12 December 2006).

Make Sure You Are Not Inadvertently Running "Spyware"

Spyware is often distinguished from "adware," that is, advertising supported software, which was designed to help shareware authors make money. There are a few examples of "good" adware, software that you can get for free if you are willing to put up with sponsored ads each time you use it. ***Good adware explicitly asks you if you are willing to accept the ads*** in exchange for the program and also promises not to share or sell any information it collects about your browsing habits.

Spyware, on the other hand, rarely asks for your permission to do what it was created to do. An exception would be something like the Google Toolbar, which offers an option to turn off data collection and, even if it is enabled, does not share its tracking data with anyone else. Spyware by definition contains some sort of tracking software that regularly tries to "phone home" via your Internet connection to report data about your browsing habits, virtually never with your explicit permission. Most spyware then sells your personal information or, worse, exploits it to attack you. To make matters worse, it is now so hard to detect spyware that even the most sophisticated users often do not realize they have been infected.[203]

Here are several ways to avoid spyware: do not download shareware or freeware, such as Kazaa, Quickclick, WebHancer, CuteFTP, etc. However, most people are going to download software at some point. If you do, try to make sure it doesn't include spyware by visiting a website that lists known spyware, such as those listed below. Be aware, however, that more and more spyware is not actively installed by users but is downloaded, installed, and run on computers using nefarious techniques such as drive-by downloads, which exploit browser features such as ActiveX.

There is software available to check your system on a regular basis for spyware. Sadly, not all such software does what it claims; instead, there are unscrupulous people who are offering "spyware detection" software that is itself spyware. Do not download any antispyware software without checking it out beforehand. There is even a website devoted to finding and exposing bogus antispyware products. Spyware Warrior Rogue/Suspect Anti-Spyware Products maintains a long and growing list of these untrustworthy products.

While you can buy good antispyware software, some of the best is available for free. Ad-Aware SE Personal Edition and Spybot Search & Destroy are excellent free utilities that detect and remove spyware. Microsoft offers its own free antispyware

[203] Leslie Walker, "Theft You Don't Even See," *Washington Post*, 1 September 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/31/AR2005083102486_pf.html> (14 November 2006).

software, Windows Defender. As of 2007, Windows Defender is only available for use on Windows XP, SP2 and Windows Server 2003, which means Windows Defender is no longer supports Windows 2000.

Most experts agree that ***there is no single product that can detect all spyware***. If I were only going to use one antispyware product on the Windows XP operating system, I would choose Windows Defender for several reasons: it has a very high detection rate; it is easy to configure; it will run automatically on a schedule; it automatically updates its detection rules; and, of course, it is free. In addition, Microsoft products tend to work very well on Windows computers.

Free Antispyware Products

Ad-Aware Spyware Checker	http://www.lavasoftusa.com/products/ad-aware_se_personal.php
Windows Defender	http://www.microsoft.com/athome/security/spyware/software/default.mspx
Spybot Search & Destroy	http://www.safer-networking.org/en/home/index.html

Antispyware Guides & Articles

11 Signs of Spyware	http://www.pcmag.com/article2/0%2C1759%2C1522648%2C00.asp
Anti-Spyware Guide	http://www.firewallguide.com/spyware.htm
Monitoring Software on Your Computer: Spyware, Adware, and Other Software, Staff Report, Federal Trade Commission, March 2005 **[PDF]**	http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf
PC Hell Spyware Removal Help	http://www.pchell.com/support/spyware.shtml
Spychecker	http://www.spychecker.com/
Spyware Guide	http://www.spywareguide.com/product_list_full.php
Spyware Warrior Rogue/Suspect Anti-Spyware Products	http://www.spywarewarrior.com/rogue_anti-spyware.htm
Spyware Watch	http://www.spyware.co.uk/
Stop Internet Abuse	http://www.celticsurf.net/webscape/abuse.html

"Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore."

Install Software and Hardware Firewalls

Whether you are using an always-on connection such as cable or DSL, or you are accessing the Internet via a dial-up connection, you need to install at least a software firewall and, I believe, a hardware firewall as well. Firewalls, while not foolproof, are the home user's best protection against Trojan horses and spyware. Both types of malware are a huge threat to the Internet community because they are insidious, hard to detect, and harder still to remove. The best advice about Trojan horses and spyware is don't get them in the first place, and firewalls remain the best defense against these types of malicious software.

Software firewalls[204] can be purchased for a relatively low price or, even better, some of the best are free. Check Firewallguide's Personal Firewall Reviews for some options.

However, while all Internet users need a software firewall, anyone with cable, DSL, or satellite Internet access needs a hardware firewall, too. The bad news is that "true" hardware firewalls are still fairly expensive and hard to configure. The good news is that there is a very inexpensive alternative for the home user that offers similar basic protection: a cable/DSL router. As with a hardware firewall, routers use Network Address Translation or NAT to hide your computer's Internet address from the bad guys. The firewall—and not your computer—becomes your connection to the Internet, making it harder for malicious hackers to see your computer, much less scan or attack it. In addition to NAT, firewalls (and good home routers) also use something called Stateful Packet Inspection (SPI) to let through only those Internet connections you request and block connections that are trying to break into your computer.

Make sure the router you purchase offers SPI and good advanced control settings. And, please, ***change your router password as soon as you install it!*** Malicious hackers know all the default logins and passwords for every router ever made. For example, check this site (just one of many):

Default Password List	http://phenoelit.darklab.org/cgi-bin/display.pl

It is important to understand that while a good home router will help protect your computer from attacks, it is not impervious. Nothing really is, but for a home user, you are going to be much more secure with software and hardware firewalls than the vast majority of users who don't do anything to protect themselves. However, in order to get the most good out of these products, you must configure them properly.

[204] The firewall that is part of Windows XP (including the improved firewall in Service Pack 2) does not provide "extrusion protection," i.e., it only detects incoming data, not data that might flow from your computer. Do not rely solely on the XP firewall.

I have compiled some of the most useful websites for learning about firewalls and routers here:

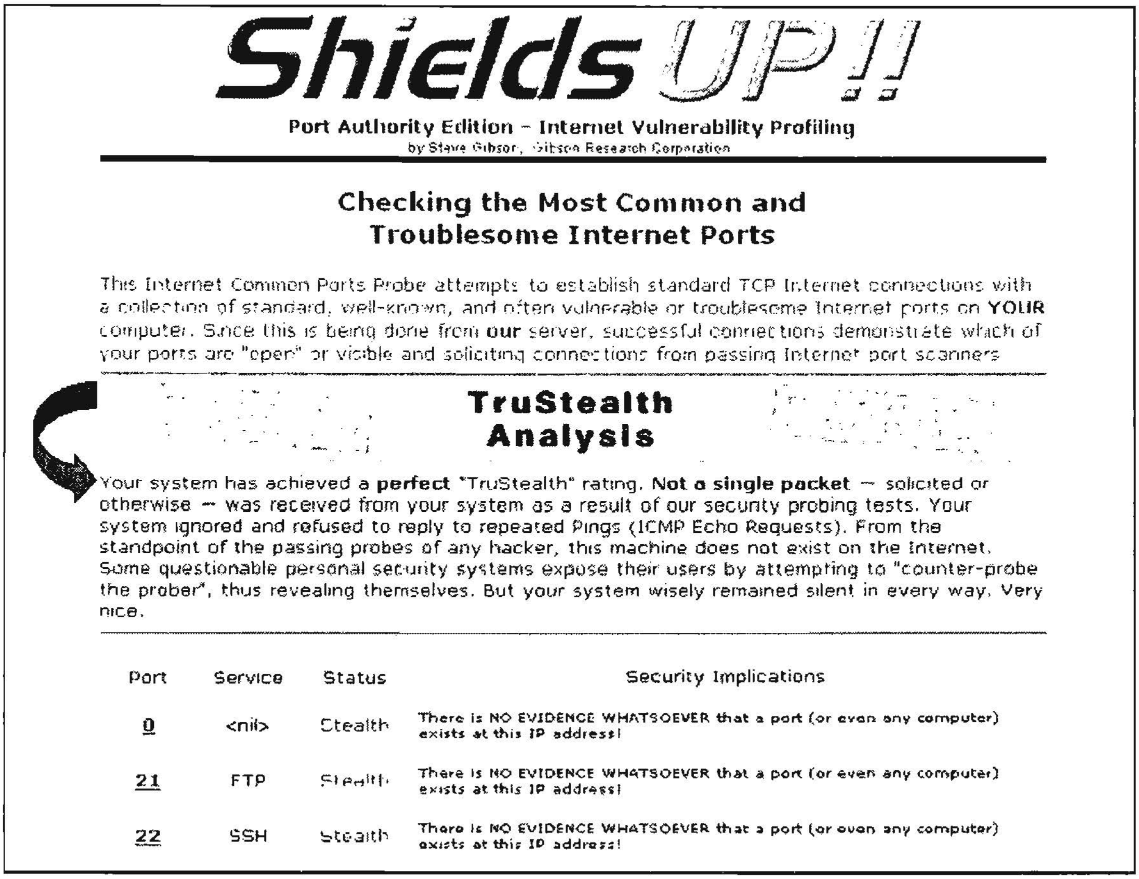
Firewallguide's Personal Firewall Reviews	http://www.firewallguide.com/software.htm
Firewallguide: Wired Routers	http://www.firewallguide.com/hardware.htm
Firewall Forensics	http://www.linuxsecurity.com/resource_files/firewalls/firewall-seen.html
Firewall Q&A	http://www.vicomsoft.com/knowledge/reference/firewalls1.html
Gibson Research's Firewall Page	http://grc.com/su-firewalls.htm
HomeNetHelp's Broadband Router Guide	http://www.homenethelp.com/router-guide/index.asp
Home Network Router Security Secrets	http://www.informit.com/articles/printerfriendly.asp?p=461084&rl=1
How Firewalls Work	http://www.howstuffworks.com/firewall.htm
Internet Firewall FAQ	http://www.interhack.net/pubs/fwfaq/
Introduction to Firewalls	http://netsecurity.about.com/od/hackertools/a/aa072004.htm
10 Steps To Make Your Firewall More Secure	http://www.itsecurity.com/features/more-secure-firewall-012207/

Free Software Firewalls for Windows

Free Personal Firewall Software	http://netsecurity.about.com/od/personalfirewalls/a/aafreefirewall.htm
Sunbelt Kerio Firewall	http://www.sunbelt-software.com/kerio.cfm Full version free for 30 days, then reverts to basic version.
Comodo Free Personal Firewall	http://www.personalfirewall.comodo.com/
Zone Alarm	http://www.zonelabs.com/

Test Your Online Security

So you installed firewall software and perhaps even hardware protection in the form of a router and you're feeling pretty smug. Before you get too comfortable, you should test your firewall to make sure it is doing the job it should be. My favorite set of tests is **Sygate/Symantec's Online Services**, which puts your computer through a whole range of scans to test its vulnerability to attack. I also recommend you run Steve Gibson's **Internet Vulnerability Profiling** at his **Shields Up!** website. This is what you want to see for every test you run at Shields Up:



Shields UP!!

Port Authority Edition – Internet Vulnerability Profiling
by Steve Gibson, Gibson Research Corporation

Checking the Most Common and Troublesome Internet Ports

This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on **YOUR** computer. Since this is being done from **our** server, successful connections demonstrate which of your ports are "open" or visible and soliciting connections from passing Internet port scanners

TruStealth Analysis

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

Port	Service	Status	Security Implications
0	<nil>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
21	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
22	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

If your computer does not pass every test, find out why and fix it. Unfortunately, every computer, like every person, is unique, so one solution definitely does not fit all. However, with a little patience and some trial and error, most vulnerabilities can be eliminated. Steve Gibson's website is especially useful in helping home users diagnose and correct computer security and privacy related problems.

Gibson's Shields Up Internet Vulnerability Profiling https://grc.com/x/ne.dll?bh0bkyd2

Sygate/Symantec Online Security Services
http://scan.sygate.com/home_homeoffice/sygate/index.jsp
Sygate is now owned by Symantec.

HackerWatch Port Scan and Simple Probe http://www.hackerwatch.org/probe/

HackerWhacker Free Tools http://whacker4.hackerwhacker.com/freetools.php
especially the Browser Leakage and Quick Scan for open ports

DSL Reports http://www.dslreports.com/tools/

PC Flank Advanced Port Scan http://www.pcflank.com/scanner1.htm

Planet Security Port Scans	http://www.planet-security.net/index.php?xid=%F7%04T%BDP%92nD
Firewall Guide: Firewall Testing	http://www.firewallguide.com/test.htm

Most personal firewalls do a decent job of blocking intruders from gaining external access a computer (i.e., *intrusion detection*). However, many of these same programs (most notably the Windows XP firewall) fail to catch applications residing on a computer that access the Internet without your knowledge or consent (i.e., *internal extrusion*). Why? Often these personal firewall packages come pre-programmed to allow some applications to pass through them without the user's knowledge. Also, it's quite easy for a malicious person to simulate a preapproved application and fool a computer into "phoning home." All that is required is to rename the malware with a commonly used file name, such as *iexplore.exe*, which is usually allowed free access to the Internet, and the attacker has opened a back door into your computer.

Check to see if your firewall passes the "leak" test by downloading Gibson's tiny Leak Test application or try one of these online firewall testers. If your firewall is properly configured (meaning you do not let programs—especially browsers—access the Internet without your permission), your firewall will pass all three leak tests. If it doesn't, you need to reconfigure your software.

Gibson Research's Firewall Leaktest	http://grc.com/lt/leaktest.htm
PCFlank Firewall Leaktest	http://www.pcflank.com/pcflankleaktest.htm
Tooleaky	http://tooleaky.zensoft.com/
Firewall Leak Tester	http://www.firewallleaktester.com/index.html

Don't Fall for the Con

Never download software or open and/or run an email attachment unless you are absolutely sure you know what it is. It used to be known as a con job and the person who committed this type of fraud a con artist. Then in the computer hacker world, the con became "social engineering, one of the most pernicious ways malware is spread. Social engineering is a con game designed to trick users into violating normal security procedures. One famous example involves a malicious user sending email that looks as though it is from a trusted source, such as "Microsoft Corporate Security Center," warning you to install the attached "fix" to a vulnerability or to go to a certain website to download a file. That "fix" is in fact a virus or some other piece of malware. Read Microsoft's policies on software distribution (they *never* distribute software directly via email) and all Microsoft downloads are from their site <http://www.microsoft.com/>.

Microsoft Policies on Software Distribution
http://www.microsoft.com/technet/security/bulletin/info/swdist.mspx

Although it is not new, another type of con called "pretexting"[205] made headlines during 2006 when some executives at Hewlett Packard got into serious trouble because of this method of obtaining information. The HP execs weren't after financial data but telephone records, and at that time it was not clear if pretexting to obtain phone records was illegal or not in the US. HP admits that it hired a firm to investigate board leaks to the press. The firm HP engaged to look into the leaks in turn hired private investigators who impersonated HP board members to get phone records belonging to at least nine reporters and one HP board member.

This is just the most high-profile complaint about the ready availability of personal records obtained by "data brokers." You need to be aware that pretexting is a widespread tactic, and the ***laws governing fraudulently obtaining non-financial personal records and information are murky at best.*** Frankly, there isn't much you can do to protect yourself from a clever and determined con artist who is going after your phone records at your phone company. The best ways to combat pretexting are laws that make pretexting a crime and companies that train their employees better.

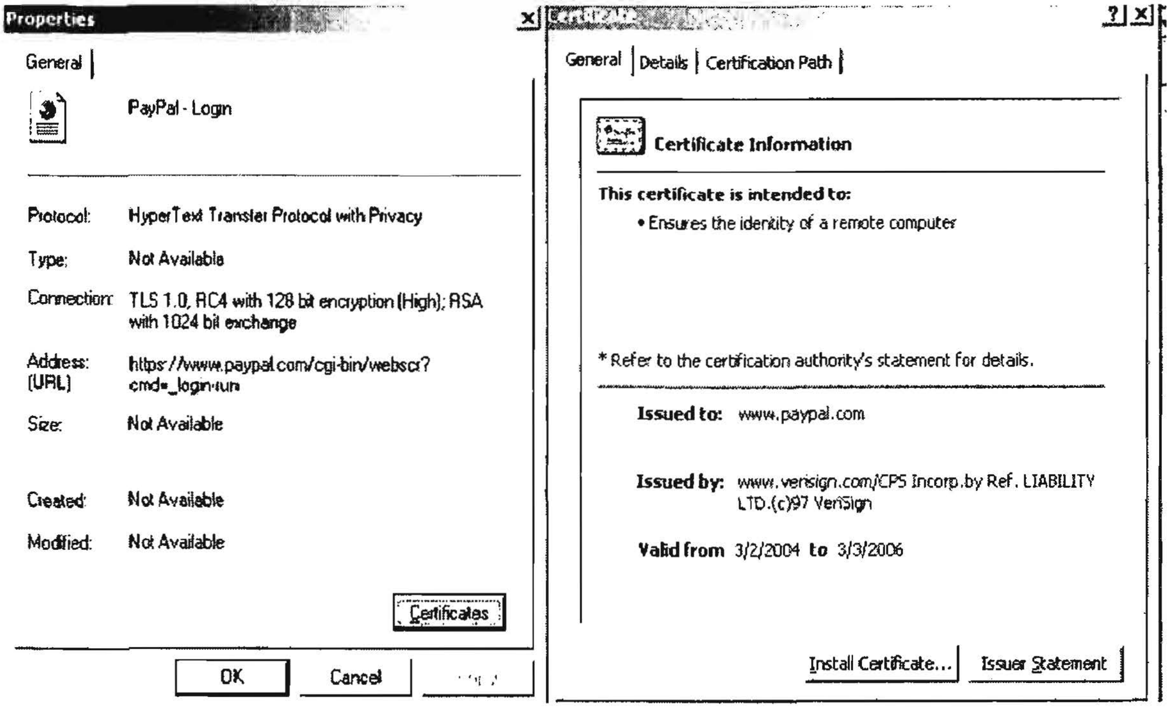
Understand Website Certificates

If you are concerned about phishing attacks and other social engineering scams, you have probably been advised to make sure the site you are visiting has a valid site certificate. And then you probably scratched your head and wondered, "how the heck can I tell if that certificate is valid or not?"

First, it is important to understand what a site certificate is and what it does for the site and for you. Any website that wants a secure connection must use encryption. In order to use encryption over the Internet, the website owner must obtain a site certificate. There are, then, two parties involved in verifying the validity of a certificate: the website owner and the trusted certificate authority. At present, your browser is probably set to recognize more than 100 trusted certificate authorities, but not all of these have the same strictness about ensuring the validity and security of

[205] The earliest use I have found of the term 'pretexting' to mean obtaining private or confidential information by pretending to be someone who has a legitimate right to or need for that information is 1980: Fair Financial Information Practices Act: Hearings Before the Subcommittee on Consumer Affairs by the United States Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on Consumer Affairs.

their data. You can check the validity of the site certificate by clicking on the locked padlock, but clever malicious hackers know how to create a fake padlock that appears to provide valid site certificate data. A more reliable way to verify a certificate is to view the webpage's *Page Info* in Mozilla or, in Internet Explorer, to right click on the webpage and select *Properties* to see, first, the general information about the page security and then, by clicking on *Certificates*, the actual certificate information such as from the PayPal website:



PayPal - Login

Protocol: HyperText Transfer Protocol with Privacy

Type: Not Available

Connection: TLS 1.0, RC4 with 128 bit encryption (High); RSA with 1024 bit exchange

Address: (URL) https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Size: Not Available

Created: Not Available

Modified: Not Available

Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.paypal.com

Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Valid from 3/2/2004 **to** 3/3/2006

In viewing the certificate information you should make sure the ***trusted certificate authority is legitimate***. If you do not recognize the name, check your browser's list of certificate authorities:

- in Firefox: Tools | Options | Advanced | View Certificates | Authorities
- in Netscape: Edit | Preferences | Privacy & Security | Certificates | Manage Certificates | Authorities
- in Internet Explorer: Tools | Internet Options | Content | Certificates | Trusted Root Certification Authorities

The certificate should have been issued to the website owner. If the ***name on the certificate*** does not match the name you expected, do not trust it.

Also look at the certificate's ***expiration date*** to make sure it has not expired.

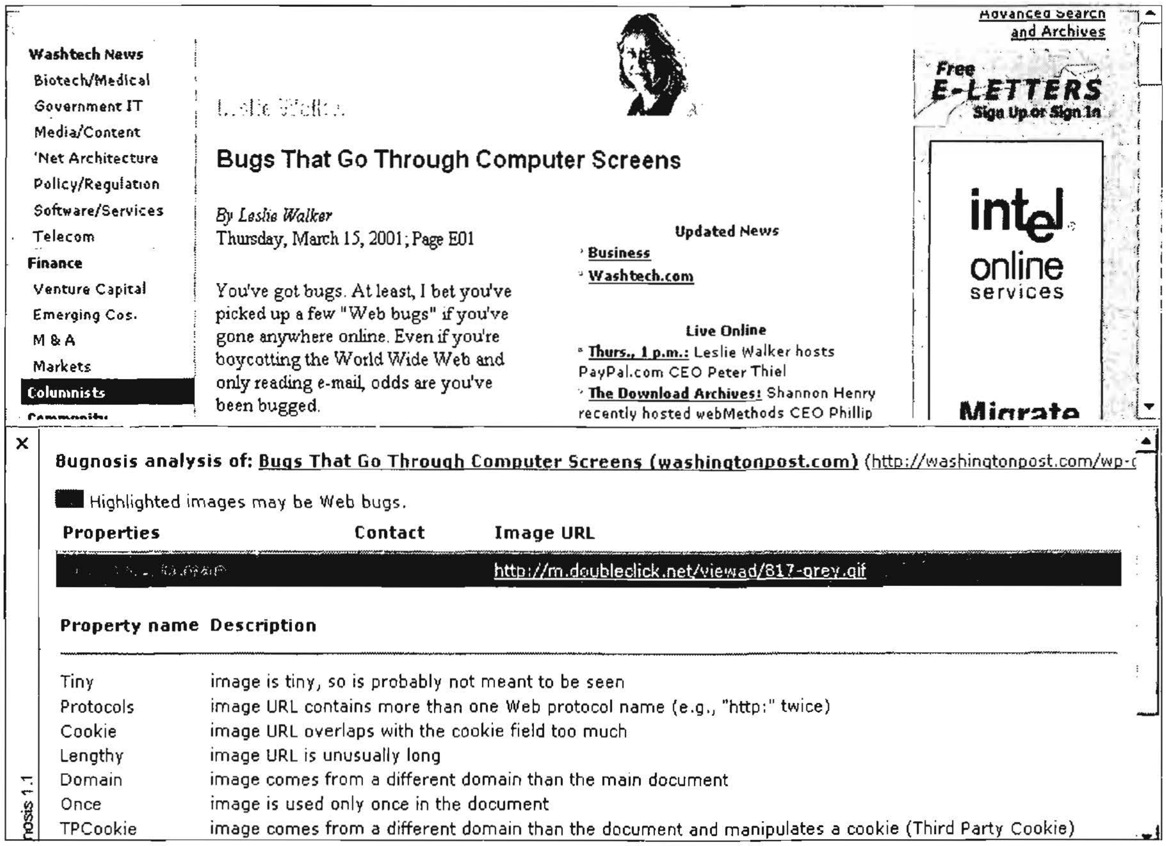
For more information on how to understand site certificates, the US CERT site has a new Cyber Security Tip addressing this topic.

Understanding Web Site Certificates http://www.us-certgov/cas/tips/ST05-010.html

---

Watch Out for "Web Bugs"

"Web bugs" are virtually invisible 1-pixel images that act as electronic tags to help websites and advertisers track users' movements across the Internet. "Also called a 'Web beacon,' 'pixel tag,' 'clear GIF' and 'invisible GIF,' it is a method for passing information from the user's computer to a third party Web site. Used in conjunction with cookies, Web bugs enable information to be gathered and tracked in the stateless environment of the Internet."[206] At present, there is no sure way to counteract all web bugs, but products are becoming available to let you "see" web bugs, block them, or remove them. All the products designed to handle web bugs must be downloaded and installed. Only products with free versions are listed here.



Leslie Walker

Bugs That Go Through Computer Screens

By Leslie Walker
Thursday, March 15, 2001; Page E01

You've got bugs. At least, I bet you've picked up a few "Web bugs" if you've gone anywhere online. Even if you're boycotting the World Wide Web and only reading e-mail, odds are you've been bugged.

Updated News
- **Business**
- **Washtech.com**

Live Online
- **Thurs., 1 p.m.:** Leslie Walker hosts PayPal.com CEO Peter Thiel
- **The Download Archives:** Shannon Henry recently hosted webMethods CEO Phillip

Bugnosis analysis of: Bugs That Go Through Computer Screens (washingtonpost.com) (http://washingtonpost.com/wp-c

■ Highlighted images may be Web bugs.

Properties	Contact	Image URL
[illegible]		http://m.doubleclick.net/viewad/817-grey.gif

Property name	Description
Tiny	image is tiny, so is probably not meant to be seen
Protocols	image URL contains more than one Web protocol name (e.g., "http:" twice)
Cookie	image URL overlaps with the cookie field too much
Lengthy	image URL is unusually long
Domain	image comes from a different domain than the main document
Once	image is used only once in the document
TPCookie	image comes from a different domain than the document and manipulates a cookie (Third Party Cookie)

Bugnosis does not block or clear web bugs, but it will certainly make you want to fumigate your computer by letting you see just how many of these pests are infesting the websites you visit, but it only works with Internet Explorer. For a detailed explanation of how web bugs work and how they are used, see the **Web Bug FAQ** provided by the Privacy Foundation.

Bugnosis	http://www.bugnosis.org/
Web Bug FAQ	http://www.bugnosis.org/faq.html
Guidescope	http://www.guidescope.com/home/
WebWasher[207]	http://www.cyberguard.com/products/webwasher/webwasher_products/classic/index.html

Find and Remove Trojan Horses[208]

There are few things worse that can happen to your computer than to become infested with a Trojan horse in general or a RAT in particular. A RAT is a special form of a Trojan: the Remote Access Trojan, which is malicious software that runs invisibly on a computer and permits an intruder to access and control that computer remotely. The reason Trojans and RATs are so pernicious, dangerous, and infuriating is that ***they are difficult to detect and harder still to exterminate***. The best defense, not surprisingly, is a good offense: don't get a Trojan in the first place. So how do most people get Trojans on their computers? There are many ways, but the most common are unwittingly installing them in games or other software, or by opening email attachments.

As if this isn't bad enough, in September 2005, F-Secure identified a new Trojan horse that moves from mobile phones to computers. It appears to be a pirated version of a mobile phone game users can download from the web; the malware installs itself and runs on a PC when a user transfers data from his mobile phone to his computer. The Trojan also infects the phone. While this vulnerability is rated as a

[206] "Web bug," *Computer Desktop Encyclopedia*. Computer Language Company Inc., 2005, *Answers.com*, <http://www.answers.com/topic/web-bug > (14 November 2006).

[207] "Cyberguard has changed the license for Webwasher Classic to Donationware and asks you to make a donation before downloading Webwasher Classic." However, the donation is voluntary.

[208] A Trojan horse is "a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage." Trojan horses are often used in what are known as "zombie" distributed denial of service attacks in which attackers place Trojans on many computers, then use them as part of a concerted attack, flooding a website or server with so much data it is effectively shut down. Many people have Trojan horses on their computers without knowing it. "Trojan horse," SearchSecurity.com, <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html> (14 November 2006).

"low" threat, it is significant because it marks the first time that malware has successfully infected both mobile devices and Windows-based computers.[209]

Trojans are hard to detect because they often use what are called "binder programs" to link them with a legitimate program so that the Trojan will execute in the background at the same time that the legitimate program runs, making the Trojan invisible to the victim.

How can you tell if you have a Trojan on your computer? Some of the telltale signs are unexplained slow performance, a CD tray that mysteriously opens and closes randomly, inexplicable error messages, strange screen images, or the computer automatically rebooting itself. These are by no means the only symptoms and, in fact, there may be no symptoms at all.

Once the Trojan has started to run, it may communicate with its home base via email, by contacting a hidden Internet chat channel, or by using a predefined TCP port, providing the attacker with the computer's IP address. Once activated, the Trojan can then be instructed to do many things, such as formatting a hard drive, sending back financial data, attacking another computer, or participating in a Distributed Denial of Service (aka "zombie") attack against a website. It gets worse. ***Trojans may have the ability to capture keystrokes***, meaning they can gather absolutely any data on a victim's computer, including passwords, credit card numbers, personal communications, files—anything you have, they have. Anything you do, they can do. Anything you see, they can see.

So how do you find and eradicate these vile vermin? First, understand that although good virus scanning software *may* detect and remove many Trojans, ***typical anti-virus scanners may not detect Trojans***. That's because Trojans use techniques to hide themselves. How then can you find out if you have a Trojan? A major clue to a Trojan infection is an unexpected open IP port, especially if the port number matches a known Trojan port. How do you find out which IP ports are open on your computer? It's easy: use the ***netstat*** utility that comes with many operating systems, including Windows. Here's how on a Windows computer:

1. disconnect the computer from the Internet
2. using Task List, close all programs that connect to the Internet (e.g., email, IM)
3. close all open programs running in the system tray

[209] Robert McMillan, "Mobile Trojan Horse Trots onto PCs," IDG News Service, PCWorld.com, 22 September 2005, <http://www.pcworld.com/news/article/0,aid,122658,00.asp> (14 November 2006).

4. open a DOS command tool and type netstat –a 15 or
   select Start | Run | netstat –a 15

Netstat will display all the active and listening IP ports on your computer refreshing every 15 seconds. What you are looking for is ***suspicious port activity***. For example, if port 31337 is active, there is a good chance you have the Back Orifice Trojan on your computer. Also, look for unknown FTP server processes (port 21) or web servers (port 80) that show up using netstat. But remember, you ***must*** disconnect from the Internet and shut down all programs that might use the Internet to get an accurate reading.

Or you can try a free online Trojan scanner such as the one available from PCFlank.com or WindowSecurity.com (below). While a negative report is no guarantee you do not have a Trojan horse, a positive test means you need to take action to remove this infection.

What should you do if you think you have a Trojan on your computer? I strongly recommend that you not start deleting software indiscriminately because something you don't recognize may in fact be a piece of vital software! Instead, if something suspicious shows up in your netstat investigation, now is the time to get some good Trojan-detection and removal software. Below are some sites that will help you locate legitimate anti-Trojan software and provide other advice on how to prevent and remediate infection.

What if you ultimately discover that your computer is infested with a Trojan? Even after you have successfully removed the malware, this may not be the end. How long was the Trojan on your system? What kind of information did it collect and forward? It is probably prudent (if inconvenient) to change all your passwords and even get new credit cards if you have used them on that computer just to be on the safe side. If you do such things as stock trading on your computer, you should probably assume your account has been compromised. In fact, assume everything on your computer has been compromised and treat the invasion as if a thief broke into your house and lived in it for months without your knowledge.

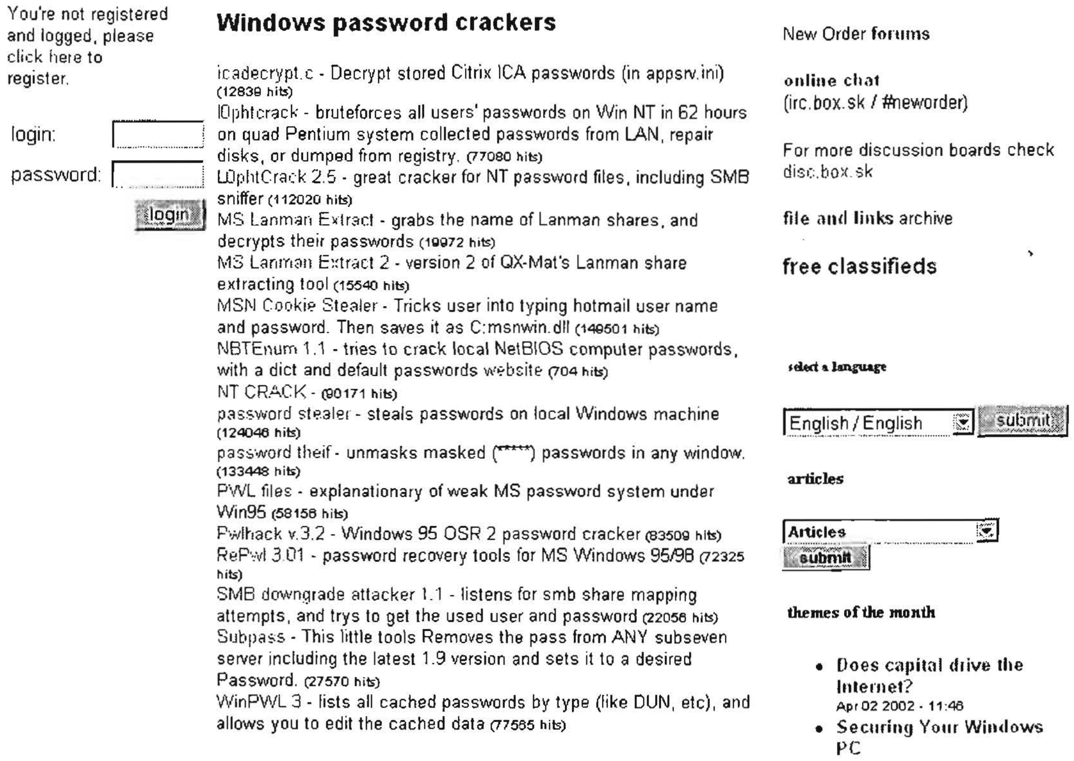
As you can see, Trojan horses are bad, really bad. Again, it is best to avoid them, and the single best defense is not to be promiscuous when it comes to downloading software and opening email attachments. The second best defense is a good firewall. But keep in mind that it is up to you to set the firewall options at a high level of protection to ensure that no Trojan can "phone home" without your permission.

List of Trojan Ports	http://secured.orcon.net.nz/portlist_list.html
Onctek's Trojan Port List	http://www.onctek.com/trojanports.html
Anti-Trojan Software Reviews	http://www.anti-trojan-software-reviews.com/
Anti-Trojan.org	http://www.anti-trojan.org/
Anti-Trojan Guide from Firewall Guide	http://www.firewallguide.com/anti-trojan.htm

PCFlank's Trojan Test Page	http://www.pcflank.com/trojans_test1.htm
WindowSecurity.com TrojanScan	http://www.windowsecurity.com/trojanscan/

Use Good Passwords

Enterprising malicious hackers and thieves are now using sophisticated programs to break passwords. Take a look at this screen shot of just one website offering Windows password crackers:



You're not registered and logged, please click here to register.

login:

password:

Windows password crackers

icadecrypt.c - Decrypt stored Citrix ICA passwords (in appsrv.ini) (12839 hits)
l0phtcrack - bruteforces all users' passwords on Win NT in 62 hours on quad Pentium system collected passwords from LAN, repair disks, or dumped from registry. (77080 hits)
L0phtCrack 2.5 - great cracker for NT password files, including SMB sniffer (112020 hits)
MS Lanman Extract - grabs the name of Lanman shares, and decrypts their passwords (19972 hits)
MS Lanman Extract 2 - version 2 of QX-Mat's Lanman share extracting tool (15540 hits)
MSN Cookie Stealer - Tricks user into typing hotmail user name and password. Then saves it as C:msnwin.dll (149501 hits)
NBTEnum 1.1 - tries to crack local NetBIOS computer passwords, with a dict and default passwords website (704 hits)
NT CRACK - (90171 hits)
password stealer - steals passwords on local Windows machine (124046 hits)
password theif - unmasks masked (*****) passwords in any window. (133448 hits)
PWL files - explanationary of weak MS password system under Win95 (58156 hits)
Pwlhack v.3.2 - Windows 95 OSR 2 password cracker (83509 hits)
RePwl 3.01 - password recovery tools for MS Windows 95/98 (72325 hits)
SMB downgrade attacker 1.1 - listens for smb share mapping attempts, and trys to get the used user and password (22056 hits)
Subpass - This little tools Removes the pass from ANY subseven server including the latest 1.9 version and sets it to a desired Password. (27570 hits)
WinPWL 3 - lists all cached passwords by type (like DUN, etc), and allows you to edit the cached data (77565 hits)

New Order forums

online chat
(irc.box.sk / #neworder)

For more discussion boards check disc.box.sk

file and links archive

free classifieds

select a language

English / English

articles

Articles

themes of the month

- Does capital drive the Internet?
  Apr 02 2002 - 11:46
- Securing Your Windows PC

While there is no guaranteed protection against a determined malicious hacker, following these basic rules probably will help protect you and not following them is an invitation to disaster:

- ➢ Never use a real word in *any* language (too easy for dictionary attacks to break).
- ➢ Never use just letters.
- ➢ Make it *at least* 8 characters long.
- ➢ Include both upper and lower case letters.

- Include numbers.
- Include special characters.

For a good article on how easy seemingly "good" passwords can be broken and how to pick a strong and memorable password, see Fred Langa's "How to Build Better Passwords" in *Information Week*.

The Simplest Security: A Guide To Better Password Practices
http://www.securityfocus.com/infocus/1537

Microsoft: How to Create Stronger Passwords
http://www.microsoft.com/security/articles/password.asp

Password Security Guide http://www.umich.edu/~policies/pw-security.html

Fred Langa: How to Build Better Passwords
http://www.informationweek.com/story/showArticle.jhtml?articleID=164303537

"Law #5: Weak passwords trump strong security."

Use Desktop Tools with Care

The past few years we have witnessed an explosion in new tools that can be downloaded for free and, in many cases, integrated into the user's browser or operating system. The highest profile of these applications was desktop search. Microsoft, Yahoo, and Ask all have some version of desktop search and there are other smaller companies such as Copernic, X1 Technologies, and Blinkx offering desktop search technology as well. However, Google's product garnered the most attention and generated the greatest controversy. According to Google, its Google Desktop is an "application that provides full text search over your email, computer files, music, photos, chats and web pages that you've viewed." Google Desktop now also indexes the entire content of PDF files and the metadata of multimedia files. In August 2005 Google introduced Google Desktop 2 in beta and dropped "Search" from its name because it does much more than just search. According to Google, "Google Desktop [2.0] doesn't just help you search your computer; it also helps you gather new information from the web with Sidebar, a new desktop feature that shows you your new email, weather and stock information, personalized news and RSS/Atom feeds, and more."[210]

What are the privacy and security concerns surrounding desktop search tools? I think Wendy Boswell, the editor of About.com's *Web Search Guide*, sums up the current state of affairs not only with Google Desktop but with all the major desktop search tools when she writes, "In a very small nutshell, the trouble with Google's Desktop Search is that when you are hooked up to a network of other computers, there are holes in Google's Desktop Search that exploit already known holes in Internet Explorer, and these two just basically open up your computer to any malicious hacker that feels like a bit of snooping."[211] Boswell points out that she uses Google Desktop Search on her own computer, but only because her computer is not networked to any others and she is has anti-virus/security/firewall protection, another backup firewall, and a broadband firewall router. And, I would add, I suspect she knows a lot more than the average user about personal computer security.

The fundamental issue with all the desktop search applications is a familiar one: balancing a very useful tool with a potential loss of privacy. "Desktop search undermines your personal security. Every time you use it, your life's an open book. Or, in this case, an open hard drive."[212] It is precisely the power and scope of desktop search tools that make them so potentially dangerous. Unlike kludgy old Microsoft Windows Explorer, which can take many minutes to search a large hard drive, desktop search tools index a hard drive upon installation and catalog the results to make retrieval very quick, usually within seconds. And desktop search tools can and do find pretty much everything on your computer, even the cache of web pages where you might have entered credit card information, for example. Which helps explain why putting desktop search tools on networked computers may not a good idea at this time. In fact, many organizations have banned the installation and use of Google Desktop, but some have discovered it came preloaded on new computers, such as one state agency that found it preinstalled on its new Dell desktops.[213]

Google's Desktop 2.0 addressed some of these security issues. Google Desktop no longer indexes or stores secure web pages or password-protected files, and the index can be encrypted. The corporate version also allows network administrators to

[210] "About Google Desktop," Google.com, <http://desktop.google.com/about.html > (14 November 2006).

[211] Wendy Boswell, "Are You Using Google Desktop Search?", About.com, 20 January 2005, <http://websearch.about.com/b/a/140602.htm?nl=1> (14 November 2006).

[212] David Sheets, "Desktop Search Threatens Your Privacy," *St. Louis Post-Dispatch*, 21 January 2005, <http://www.stltoday.com/techtalk> (article no longer available).

[213] C.J. Kelly, "Google Desktop - Yet Another Security Frightener," Computerworld, 28 December 2006, <http://www.techworld.com/features/index.cfm?featureID=3066&printerfriendly=1> (5 February 2007).

restrict the indexing of specific files. Nonetheless, users who have registered with Google—for example, Gmail account holders—should have more concerns because of the potential for Google to "connect the dots" and create a detailed profile of its registered users.[214]

Google Desktop is not alone in creating concern for security experts. All desktop search tools are inherently problematic, but Microsoft's desktop search tool is probably the most worrisome because it launches ActiveX in Internet Explorer, and ActiveX controls are among the most notoriously vulnerable applications on the web. Neither Microsoft nor Yahoo integrates web and local desktop search as Google does (yet). However, users can limit the Google Desktop to searching the hard drive, disabling the web search feature and thus gaining a measure of security. To do so, users need to make a decision during the setup. At the end of the setup process, Google Desktop asks you to enable or disable "Advanced Features." Enabling Advanced Features "sends Google non-personal data about how you're using the program, along with reports if it ever crashes. It also sends information about the websites you visit so that Sidebar can show personalized info, such as personalized news. Analyzing this data from many users helps our engineers better understand how people actually use Google Desktop and therefore how we can improve it. If you don't want Google Desktop to send this information, simply uncheck the Advanced Features checkbox. Desktop will immediately stop sending any of this non-personal information to Google."[215] You should also uncheck the option to keep your local files and cached web pages permanently out of your Google web search results; this option is under "Google Integration" in the Preferences window.

Search expert Danny Sullivan offers a very good and measured assessment of desktop search, in particular Google Desktop, in which he offers sensible advice for keeping your data safe and private while still enjoying the benefits of desktop search.

Danny Sullivan, "A Closer Look at Privacy and Desktop Search,"
SearchEngineWatch.com, 14 October 2004,
http://searchenginewatch.com/sereport/article.php/3421621

[214] Elinor Mills, "Google Balances Privacy, Reach," *CNET News*, 14 July 2005, <http://news.com.com/Google+balances+privacy%2C+reach/2100-1032_3-5787483.html> (14 November 2006).

[215] Google Desktop Features, <http://desktop.google.com/features.html#senddata> (14 November 2006).

Protect Yourself from Search Engine Leaks

In late July 2006, AOL published a list of 20 to 36 million search inquiries collected over a three-month period that included identification numbers for 658,000 unnamed users at their now defunct Research website <http://research.aol.com/>. It didn't take long for some fairly bright researchers to piece together some of the information and come up with real people whose queries were released. This was possible largely because AOL kept individual user's queries together in order to show the pattern of a person's searches over a period of time. "Searches by individual users are grouped together, often forming small profiles of a user's habits and interests. The files include the date and time of each inquiry and the address of the Web site the user chose to visit after searching."[216]

Why would AOL do such a thing in the first place? AOL's intention was to provide useful data to researchers performing "search research." However, the data turned out to be more "helpful" than AOL intended. If you think about it, how much effort does it take to figure out a specific user's name and location if you have three months of his or her searches? And since all the queries also included a date/time stamp and the link to the site they visited from AOL, there are other ways a site manager could use site logs to put together a profile on someone. What some truly enterprising person or group could do with this data is limited only by their imagination. Once the news came out that individuals could be identified from the database, AOL took the data off its website, but of course it was too late. Sites mirroring the database immediately popped up.

The lessons to be drawn from this episode are too many to name, but at the very least we know that what we like to think of as privacy is largely an illusion and what seems like an innocent act of "openness" and "sharing" can backfire in the worst possible way. What can you do to protect yourself against disclosures such as the one described above or from inadvertent leaks of search engine data? I have repeatedly warned people about using search services that require you to log into the site. AOL, Google, Live, and Yahoo all offer such services, which illustrate my rule of thumb: anything that adds convenience brings with it some degradation of privacy and/or security. The fact is that ***you are personally identifiable if you have an account with a search engine site***.

But what is the risk that you can be identified from your searches if you do not have an account at a search site? In light of the AOL incident, *Wired* updated a January 2006 article on this topic, and some of the points they make are as follows:

[216] Saul Hansell, "AOL Removes Search Data on Group of Web Users," New York Times, 8 August 2006, <http://www.nytimes.com/2006/08/08/business/media/08aol.html> (archived article requires payment).

> "How does a search engine tie a search to a user?
>
> If you have never logged in to a search engine's site, or a sister service like Google's Gmail offering, the company probably doesn't know your name. But it connects your searches through a cookie, which has a unique identifying number. Using its cookies, Google will remember all searches from your browser. It might also link searches by a user's internet protocol address.
>
> How long do cookies last?
>
> It varies, but 30 years is about average. AOL drops a cookie in your browser that will expire in 2034. Yahoo used to set a six-month cookie but now its tracker expires in 2037. A new cookie from Google expires in 2036.
>
> What if you sign in to a service?
>
> If you sign in on AOL, Google or Yahoo's personalized homepage, the companies can then correlate your search history with any other information, such as your name, that you give them. If you use their e-mail or calendar offerings, the companies can tie your searches to your correspondence and life activities. Together these can provide a more complete understanding of your life than many of your friends or family members have.
>
> Why should anyone worry about this leak or bother to disguise their search history?
>
> Some people simply don't like the idea of their search history being tied to their personal lives. Some people check to see if their Social Security or credit card numbers are on the internet by searching for them. Ironically, for more than a few AOL users, the leak of the search terms means that this sensitive information is now on the web."[217]

One of the things the *Wired* article recommends is cookie management. The problem is that unless you routinely refuse all cookies, it is very difficult to avoid some risk of identification, however small that risk may be. Using the Internet without using any cookies is not a realistic option for most of us most of the time, so we have to find a reasonable balance between no cookie use and wide open acceptance of all cookies. Luckily, browsers have gotten much better in the way they permit users to manage cookies. Refer to the section on Managing Your Cookies for details on how to minimize problems with cookies. The *Wired* article also mentions more sophisticated options for protecting your privacy, such as anonymizers and proxy services. None of these comes without a downside or is a guarantee of privacy.

The best approach is to be prudent by limiting your use of cookies via browser settings and/or third-party software to "crunch" cookies. Also, ***never search for personal data, such as your social security or credit card number at any site***

[217] Ryan Singel, "FAQ: AOL's Search Gaffe and You," Wired, 11 August 2006, <http://www.wired.com/news/politics/privacy/1,71579-2.html> (14 November 2006).

where you are registered or logged in, e.g., if you use personalized Google, AOL, Yahoo, Live, etc. If you do, you can be sure there is a record of that search. If you want to run these types of searches, the best thing to do is to block cookies for that search session, then clean out your browser's cache. That way, your search will not be stored anywhere and there will be no "cookie trail" at any site.

A number of articles recently have touted **IxQuick**, a metasearch engine, as an alternative search engine because IxQuick does not keep records of searchers' IP addresses. According to the company, "We have a program running which opens the log files and deletes the user IP addresses and overwrites them...[and] the company removes the unique ID from Ixquick.com's cookies."[218] Of course, you still must place your trust in this Amsterdam-based company not to change their policy or make a mistake. Another option to consider is Clusty, a superb search service based on Vivisimo's technology. Clusty says, "We at Clusty don't track you. Our toolbar doesn't track you. We don't want to know your email address." <http://clusty.com/privacy>

IxQuick	http://ixquick.com/
Clusty	http://clusty.com/

Finally, I also want to mention an article that includes more drastic measures one can take to keep searches private. The focus of the article is Google, but many of the suggestions work with other search engines. *I am not recommending or endorsing any of the software mentioned in the article*, but I thought you should know of other options.

Amit Agarwal
"How to Stop Google from Recording Your Search Habits"
Digital Inspiration, 13 August 2006,
http://labnol.blogspot.com/2006/08/how-to-stop-google-from-recording-your.html

Think Twice Before Registering at Search Sites

During the summer of 2005 Google became upset over an article[219] in CNET News demonstrating how much information the author could find about Google CEO Eric Schmidt using—you guessed it—Google. All the information the CNET reporter

[218] Declan McCullagh, "FAQ: Protecting Yourself from Search Engines," CNET News, 9 August 2006, <http://news.com.com/2102-1025_3-6103486.html?tag=st.util.print> (14 November 2006).

[219] Elinor Mills, "Google Balances Privacy, Reach," CNET News, 14 July 2005, <http://news.com.com/Google+balances+privacy%2C+reach/2100-1032_3-5787483.html> (14 November 2006).

found was from publicly available sources only. While that is interesting and not surprising, far more intriguing are the observations in the article about what she could have found had the reporter had access to Google's databases.

> "Assuming Schmidt uses his company's services, someone with access to Google's databases could find out what he writes in his e-mails and to whom he sends them, where he shops online or even what restaurants he's located via online maps. Like so many other Google users, his virtual life has been meticulously recorded."[220]

It's not just Google, of course, that collects personal data from ***registered users***. Yahoo, Live Search, A9, and other search services offering registration, online businesses, etc., also collect personal information when you register with them. But Google has so much of the current market share they are the highest profile company in terms of privacy concerns. "Kevin Bankston, staff attorney at the Electronic Frontier Foundation, said Google is amassing data that could create some of the most detailed individual profiles ever devised."[221] How does this happen?

> "As is typical for search engines, Google retains log files that record search terms used, Web sites visited and the Internet Protocol address and browser type of the computer for every single search conducted through its Web site. *[comment: this is true of any website you visit: any site can gather limited, non-personally identifying information that is readily available from the browser.]*
>
> In addition, search engines are collecting personally identifiable information in order to offer certain services. For instance, Gmail asks for name and e-mail address. By comparison, Yahoo's registration also asks for address, phone number, birth date, gender and occupation and may ask for home address and Social Security number for financial services."[222]

The danger lies in the ability to put together all these pieces of data to create a personal profile: "If search history, e-mail and registration information were combined, a company could see intimate details about a person's health, sex life, religion, financial status and buying preferences."[223] ***Simply using Google or any other search engine to search poses little privacy risk*** because of the sheer volume of traffic at these sites and the lack of any personal data about the searcher. ***The real privacy concerns arise when someone is a registered user*** at a site such as Google, Yahoo, AOL, Live Search, or A9. In theory, the information collected and stored about a user could enable someone to put together a remarkably thorough profile of that individual user.

[220] Mills.

[221] Mills.

[222] Mills.

[223] Mills.

Both the original CNET article and the Newsfactor article[224] make a good case for why users should either not register at sites such as Google, Yahoo, AOL, Live Search, and A9. However, if you do register, then you should consider using one browser for web searches and another for services such as the search engine's email, toolbar, instant messaging, etc. While there are no known abuses of this information as of now, who knows what the future holds or, worse, what could happen if unscrupulous persons got their hands on this data. This is something to keep in mind, especially when using search engines in the workplace.

Take Care with ZabaSearch

A new people search service called ZabaSearch opened during 2005 and caused an immediate firestorm. This was somewhat surprising given that it is only one more among many such sites offering personal data, but ZabaSearch has been the catalyst for a lot of anger and frustration about our ever-shrinking privacy. One reason ZabaSearch garnered so much attention is because it is offering some of its tantalizing data for free, unlike most services that charge for the same information. But the main reason ZabaSearch captured so much attention is it is the focus of one of those panicky emails warning people about its dangers. While the essence of the email is true, it is misleading because it encourages people to think ZabaSearch is something new, special, or unique. If one were truly cynical, one might even suspect ZabaSearch of being behind those spam mailings as a way of getting people to ask to have their data removed.

I need to emphasize this: ***do not try to have your data removed from ZabaSearch***. ZabaSearch says:

> "If you are interested in creating, editing or deleting records, please submit a valid e-mail address below and we will send you specific instructions on how to do that. Please make sure you can receive e-mail from the ZabaSearch.com domain to insure you receive our reply."[225]

People who have tried to remove their information from ZabaSearch have discovered that ZabaSearch demands they provide even more detailed information about themselves than ZabaSearch already has access to (purportedly on the grounds that they have to ensure you are really who you claim to be). ZabaSearch does not view itself as responsible for the information it provides because it does not own that information. ***All of ZabaSearch's data comes from public databases***

[224] Jack M. Germain, "Google Has Your Data: Should You Be Afraid?" Newsfactor Network, 17 August 2005, <http://www.newsfactor.com/story.xhtml?story_id=37466> (15 November 2006).

[225] ZabaTools, ZabaSearch.com, <http://www.zabasearch.com/thankyou.php> (14 November 2006).

maintained by such entities as state, local, and even the US government. Most of this type of data simply cannot be removed from the public record.

If you think we can stop companies like ZabaSearch, think again. As attorney Anita Ramasastry, points out, "[I]n a recent court case, the First Amendment has been held to allow publication *even when it predictably will threaten the safety of particular individuals.* Threats themselves can be made criminal, consistent with the First Amendment. But when information is not itself a threat—but does pose one—courts have recently tended to allow the information to be published, even on the Internet."[226] [*emphasis added*] Ramasastry goes on to say that, in her opinion, sites providing this detailed kind of personal information should be regulated. However, at present only medical records are afforded the kind of legal protection many people would like to see extended to other types of information, e.g., bankruptcy records, divorce data, real estate transactions. As of now, this information is fair game, our privacy is under assault, and the balance of power is on the side of the First Amendment: "...when constitutions do protect privacy, they typically protect it against invasion by the government—not by other citizens. Meanwhile on the other side of the balance, the First Amendment protects a person's right to speak and publish information, absent a compelling governmental interest in silence. So while *privacy rights don't help those who find themselves the subject of digital dossiers,* free speech rights do help the dossier-makers."[227] This is a difficult issue and one the Founders could hardly have imagined because the concepts of things like computers, the Internet, and online identity theft were simply unimaginable for them.

Can You Opt Out of Online Directories?

Many people are interested in (in some cases, desperate to) get their personal information out of the many online directories that now brazenly sport that data. The Privacy Rights Clearinghouse offers a very useful webpage on this subject, including a handy chart of the major "data vendors" who do and who do not offer opt out provisions. The prospect of getting your personal information out of the many databases is daunting and some of the procedures are highly dubious. For example, to get your data out of PeopleFinders, you are required to provide the following information:

> Complete Social Security number, First name, Last name, Middle initial, Aliases and A.K.A.'s, Complete current address, Complete former addresses going back

[226] Anita Ramasastry, "Can We Stop ZabaSearch—and Similar Personal Information Search Engines?: When Data Democratization Verges on Privacy Invasion," FindLaw.com, 12 May 2005, <http://writ.news.findlaw.com/ramasastry/20050512.html> (14 November 2006). .

[227] Ramasastry.

20 years , Date of Birth - including month, day, and year. Include print out of info. to be removed.

If you actually provide this much detailed data, you may be opening yourself up to identity theft. Furthermore, the Privacy Rights' page identifies twenty data vendors who offer opt out policies and fifteen that do not. All the vendors who allow users to try to remove personal information have their own procedures and requirements, and even if you diligently follow all these steps and these vendors really do remove the data, this still leaves many more vendors who will not remove your data as well as new vendors, unknown vendors, and foreign vendors. However, that's not the worst of it: "Opting out may prove to be a fruitless venture since often online vendors will simply repopulate the data when they obtain their next download of information from the source. According to People Data, their information is refreshed every three to four months. Your only option would be to check back and go through the opt-out process again if you find your information has been reposted."[228] ***Unless and until there is a way to get personal information out of public databases, requesting online data brokers to remove your information is probably counterproductive.***

In short, trying to keep your personal data private will quickly turn into a full-time job, you almost certainly will not fully succeed, and you will have to keep asking to have your data removed over and over again. So what are we to do? If you are a victim of domestic violence, stalking, or some other such crime, it is worth your time and energy to try to keep your personal information off the Internet and out of these databases. For the rest of us, prevention is the best approach. Guard your "holy trinity" of personal data—name/date of birth, address, and Social Security Number. Be especially leery of providing your Social Security Number. Most companies want your business, and if you refuse to provide an SSN, they probably will still do business with you rather than lose a customer. For now, it appears we are going to have to live with the uneasy balance between privacy and the free flow of information.

Understand the Pros and Cons of an Anonymizing Proxy

If you are truly concerned about revealing anything about yourself as you surf the web, consider using an anonymizing proxy. A proxy is an agent that interfaces between you and the Internet. Most proxies strip out all references to your IP address, your location, your email, types of software you are using, and the previously visited page (http-referrer). Some, such as **Anonymizer**, also let you block cookies and disable scripts, both of which can potentially be used to track your

[228] "Online Data Vendors: How Consumers Can Opt Out of Directory Assistance and Non-public Information," Privacy Rights Clearinghouse, February 2006, <http://www.privacyrights.org/ar/infobrokers.htm> (12 September 2006).

movements on the web or disclose information about you. ***One of the big drawbacks with many proxy services is that you may be identified as using an anonymizing proxy, which could "flag" you as someone to watch. Also, keep in mind that you are not anonymous to the proxy provider.***

Most anonymizing services are strictly "http" proxies, which means they only give you "anonymity" when browsing webpages, which is all you need most of the time. My experience with proxies is that they *probably will slow you down*. Several years ago there were documented problems with anonymizers that allowed websites to view your real IP address. These bugs have largely been fixed but if you are using any of these services, *be sure to turn off JavaScript, Java, and ActiveX controls in your browser*. Check privacy guru Richard Smith's Computerbytesman page to test any anonymizing service for leaks.

Finally, anonymizing proxies may create a *false sense of security* that in itself can be dangerous. One experimental Trojan horse program, Setiri, actually disguises itself as Internet Explorer, connects to a website via Anonymizer.com, and uses Anonymizer to execute commands from the victim's computer. Once connected the Trojan can download programs, such as keystroke monitoring software, and steal any data on that computer, sending it via Anonymizer so it cannot be traced.[229] While the Setiri Trojan does not exploit a flaw in Anonymizer, it does point to how malicious users can turn good things to evil purposes.

Warning: Never use an anonymizing proxy that requires registration to use a **free** service! Some proxies have been associated with people and organizations that want to gather information about users.

InfoAnarchy's Anonymous Web Searching
http://www.infoanarchy.org/en/Anonymous_Web_Surfing

Free Web Anonymizer Services http://www.cexx.org/anony.htm

Web Anonymizing Services http://www.computerbytesman.com/anon/index.htm

Test Page for Web Anonymizing Services
http://www.computerbytesman.com/anon/test.htm

"Law #9: Absolute anonymity isn't practical, in real life or on the web."

[229] Kim Zetter, "Trojan Horse Technology Exploits IE," PCWorld.com, 5 August 2002, <http://www.pcworld.com/news/article/0,aid,103620,tk,wb081202x,00.asp> (14 November 2006).

Convert with Caution

As part of its initiative to enhance software security and share this information with users, the National Security Agency's Information Assurance Directorate published a new guide in December 2005: "Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF." This is a very important issue because failure to redact documents properly—whether they are declassified government documents, court records, proprietary company documents—can lead not just to embarrassment but also to very serious security violations and potential risks to individuals. I call your attention to the very sad case in May 2005 in which an improperly prepared PDF document about the killing of the Italian intelligence agent Nicola Calipari in Iraq was quickly discovered and exploited by the press worldwide. Not only was classified information leaked to the world, but the lives of those whose identities were revealed were also put in jeopardy by the improper method of removing data from a MS Word file and converting it to PDF. This is an important guide and I urge you to keep a copy for yourself and your organization.

"Redacting with Confidence: How to Safely Publish Sanitized Reports Converted
from Word to PDF"
Architectures and Applications Division of the Systems and Network Attack Center
(SNAC)
Information Assurance Directorate, National Security Agency
last updated 2 February 2006
http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1

For details on the Calipari incident and the ensuing disclosure of classified information, I recommend an article from the Times Online (UK).[230]

Your privacy and security are only as good as the weakest link using your computer (a spouse, a child, or your teenager's friends...)

[230] Simon Freeman, "Italy Releases Report into Death of Security Agent," Times Online, 2 May 2005, <http://www.timesonline.co.uk/article/0,,7374-1594880,00.html> (14 November 2006).

Always Put Privacy and Security Before Convenience

Remember the quote from Scott MacNealy? It is tempting to store credit card and password information on your hard drive or let a site retain your credit card number or log you in automatically. I highly recommend you eschew these conveniences and force yourself to ***enter sensitive information every time you need to use it and only when it is absolutely necessary***. Do not volunteer information about yourself and only fill in the required boxes on forms. An enterprising thief can break into your computer, steal the contents of it, and get out without your ever knowing he was there. Also, if you don't store credit card information at websites, that data won't be sitting in a database potentially waiting to be stolen. Every time you do something new or different on the Internet or your computer, ask yourself if it could potentially compromise your privacy or security, then decide if the benefits outweigh the risks before proceeding.

"Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore."

General Security & Privacy Resources

The best defenses against the many dangers lurking on the Internet are awareness and information. Because security and privacy threats are so pervasive and increasing in number and potency, staying on top of threats and means of protection is crucial.

Steve Gibson, rightly famous for his Shields Up! website and free software (e.g., "UnPlug n' Pray"), launched a new service with TechTV's Leo Laporte in 2005. Every Thursday afternoon they create a 20-25 minute audio column about personal computer security called "Security Now!" The topics covered include personal passwords (a must read), NAT routers as firewalls (another must read), "HoneyMonkeys" (no, I'm not making that up), unbreakable WiFi security, and bad WiFi security. The audio broadcasts are archived in several formats, including a text file, a PDF version, and an HTML webpage. There is also an option to receive an email reminder whenever the page is updated. Gibson has the ability to cut through the jargon to explain these topics clearly and to offer practical advice on how to handle personal computer security issues.

Security Now! http://www.grc.com/securitynow.htm

The following are a few more of the many excellent sites providing news, information, and advice on Internet privacy and security.

Center for Privacy and Technology Ten Ways to Protect Privacy Online	http://www.cdt.org/privacy/guide/basic/topten.html
EPIC Online Guide to Privacy Resources	http://www.epic.org/privacy/privacy_resources_faq.html
Georgi Guninski Security Research	http://www.guninski.com/
Security Focus	http://www.securityfocus.com/
Yahoo News Computer Security	http://fullcoverage.yahoo.com/fc/Tech/Computer_Security
Yahoo News Cybercrime and Internet Fraud	http://news.yahoo.com/fc/Tech/Cybercrime_and_Internet_Fraud/
Yahoo News Internet Privacy	http://news.yahoo.com/fc/Tech/Internet_Privacy/

Conclusion

The overall implications of the Internet for how we work and how we play are just beginning to be discussed and understood. The Internet is changing, or at the very least touching, people's lives in ways we have not imagined. I close with an example of the reach of the web. My 97-year-old aunt in South Carolina had a bit part in an obscure movie in 1989. Despite the fact that the movie has been largely forgotten, my aunt has an "Actress Filmography" in the Internet Movie Database. She, of course, was unaware of her Internet presence and was both thrilled and more than a little shocked to find that even she was "in cyberspace."

The point, of course, is that no one is out of reach of this powerful, invasive technology. We change the world with our technology and we, in turn, are altered by that same technology. It remains to be seen where our technology leads us, whether into an "endless frontier"[231] or, more ominously, into a "cemetery of dead ideas."[232]

[231] Vannevar Bush, *Science: The Endless Frontier,* Washington, D.C.: United States Government Printing Office, 1945.

[232] Miguel de Unamuno, *The Tragic Sense of Life,* Princeton: Princeton University Press, 1990. (November 2005), p. 100.

Web Sites by Type

General Purpose Search Engines

A9	http://a9.com/
Ask	http://www.ask.com/
Exalead	http://www.exalead.com/search
Gigablast	http://www.gigablast.com/
Google	http://www.google.com/
Live Search	http://www.live.com/
Yahoo	http://search.yahoo.com/

Directories

Best of the Web	http://botw.org/default.aspx
Galaxy	http://www.galaxy.com/
Google Directory	http://directory.google.com/
Open Directory	http://dmoz.org/
Yahoo Directory	http://dir.yahoo.com/

Metasearch Sites

Open Directory's List of Metasearch Sites	http://dmoz.org/Computers/Internet/Searching/Metasearch/
Clusty	http://clusty.com/
Dogpile	http://www.dogpile.com/
Ithaki	http://www.ithaki.net/indexu.htm
IxQuick	http://www.ixquick.com/
Jux2	http://www.jux2.com/
Mamma	http://www.mamma.com/
Metacrawler	http://www.metacrawler.com/
The Pandia Metasearch Engine	http://www.pandia.com/metasearch/index.html

Search.com	http://www.search.com/
Surfwax	http://www.surfwax.com/

Megasearch Sites

All Search Engines	http://www.allsearchengines.com/
Find It Quick	http://www.quickfindit.com/Search_Engines/
Search—22	http://www.search-22.com/
SearchEzee	http://www.searchezee.com/search.shtml

Internet Guides and Tutorials

BrightPlanet's Guide to Effective Searching of the Internet	http://www.brightplanet.com/deepcontent/tutorials/search/index.asp
Finding Information on the Internet: A Tutorial	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/FindInfo.html
Internet Tutorials from University of Albany Libraries	http://www.internettutorials.net/
Internet Scout Report	http://scout.wisc.edu/Projects/PastProjects/toolkit/searching/index.html
Intute: Virtual Training Suite	http://www.vts.intute.ac.uk/
Pandia's Goalgetter	http://www.pandia.com/goalgetter/index.html
Phil Bradley's Searching the Internet	http://www.philb.com/searchindex.htm
Search Engine Watch Tutorials (old but still useful)	http://www.searchenginewatch.com/resources/article.php/2156611
Web Search Guide	http://www.websearchguide.ca/tutorials/tocfram.htm

Google Help & Tools

Google Help	http://www.google.com/help/features.html
Google Guides	http://www.google.com/press/guides.html
Google Book Search	http://books.google.com/
Google Language Tools	http://www.google.com/language_tools
Google Scholar	http://scholar.google.com/
Google International Sites	http://www.google.com/language_tools
Google Blog Search	http://blogsearch.google.com/
Google Patent Search	http://www.google.com/patents

Google Directory	http://directory.google.com/
Google SMS	http://www.google.com/sms/
Google Scholar	http://scholar.google.com/
Google Trends	http://www.google.com/trends
Google Find Related Images	http://blog.outer-court.com/related/
Simply Google	http://www.usabilityviews.com/simply_google.htm
Google Rankings	http://www.googlerankings.com/kdindex.php
Google Compare	http://oy-oy.eu/google/world/

Specialized Search Tools

Answers.com	http://www.answers.com/
Babelplex	http://www.babelplex.com/
Fagan Finder Search by File Type	http://www.faganfinder.com/filetype/
Google Trends	http://www.google.com/trends
Neighborsearch	http://www.blog.outer-court.com/neighborsearch/
OAIster	http://www.oaister.org/
Searchroller	http://www.researchbuzz.org/2004/10/new_yahoo_hack_searchroller_fo.shtml
The Wayback Machine	http://web.archive.org/
Yahoo Proximity Search	http://www.researchbuzz.org/2004/10/ynaps_yahoo_nonapi_proximity_s.shtml

Custom Search Engines

Gigablast's Custom Topic Search	http://www.gigablast.com/cts.html
Google Custom Search Engine	http://www.google.com/coop/cse/overview
Yahoo Search Builder	http://builder.search.yahoo.com/
Windows Live Search Macros	http://search.live.com/macros/default.aspx
Rollyo	http://rollyo.com/
Eurekster's Swicki	http://swicki.eurekster.com/
PSS	http://www.pssdir.com/
Alexa Web Search Platform	http://websearch.alexa.com/welcome.html

Subject Guides, Virtual Libraries, and Reference Desks

About	http://www.about.com/
Encyclopedia.com	http://www.encyclopedia.com/
Encyclopedia Britannica[233]	http://www.britannica.com/
Hotsheet	http://www.hotsheet.com/
INFOMINE	http://infomine.ucr.edu/
Information Please	http://www.infoplease.com/
Intute (formerly RDN)	http://www.intute.ac.uk/
The Internet Public Library	http://www.ipl.org/
Librarians' Index to the Internet	http://lii.org/
The Library Spot	http://www.libraryspot.com/
Martindale's The Reference Desk	http://www.martindalecenter.com/
My Virtual Reference Desk	http://www.refdesk.com/
Pinakes Subject Gateway[234]	http://www.hw.ac.uk/libWWW/irn/pinakes/pinakes.html
Wikipedia	http://en.wikipedia.org/
WWW Virtual Library	http://vlib.org/Overview.html
Yahoo Reference	http://education.yahoo.com/reference/

Wikipedia and Wikipedia Search

Wikipedia	http://en.wikipedia.org/
Search Web Links at Wikipedia	http://en.wikipedia.org/w/index.php?title=Special%3ALinksearch
Clusty's Wikipedia Search (English only)	http://wiki.clusty.com/
FUTEF (Beta)	http://futef.com/
Qwika	http://www.qwika.com/
LuMriX	http://wiki.lumrix.net/
Wikiseek	http://wikiseek.com/
WikiWax	http://www.wikiwax.com/

[233] Although full-text articles require a paid subscription to *Encyclopedia Britannica*, the site is still a useful starting place for research and includes free access to the *Britannica Concise Encyclopedia*.

[234] Pinakes is the gateway to EEVL and dozens of other equally valuable specialized research sites.

Best Mapping Sites

Ask Maps	http://maps.ask.com/maps
France Telecom's Pages Jaunes	http://photos.pagesjaunes.fr/
Google Earth (must be downloaded)	http://earth.google.com/
Google Maps	http://maps.google.com/
Map24	http://www.map24.com/
MapQuest	http://www.mapquest.com/
Maporama	http://www.maporama.com/share/
Mappy's Aerial Photos	http://www.mappy.com/ (select Maps | Aerial Photos)
Multimap (excellent source of maps worldwide)	http://www.multimap.com/
Spain's Callejero Fotographico	http://www.qdq.com/indexfotos.asp
Mappy (Europe)	http://www.mappy.com/
ViaMichelin (Europe, US, Canada)	http://www.viamichelin.com/viamichelin/gbr/dyn/controller/Maps
Windows Live Local/Virtual Earth	http://local.live.com/
Windows Live Spaces/Virtual Earth	http://virtualearth.spaces.live.com/
Yahoo Maps	http://maps.yahoo.com/

Best Map MetaIndices

About's Maps	http://geography.about.com/science/geography/msub1.htm
Martindale's "Virtual" Geoscience Center	http://www.martindalecenter.com/GradGeoscience_5_GG.html
Odden's The Fascinating World of Maps and Map-Making	http://oddens.geog.uu.nl/index.html
Perry-Castaneda Library Map Collection at the University of Texas Austin	http://www.lib.utexas.edu/Libs/PCL/Map_collection/map_sites/map_sites.html
ReisWijs Route Planner Metasite	http://www.reiswijs.co.uk/routeplanner/routeplanner.html

Book Search

A9 (select "books by Amazon")	http://www.a9.com/
Amazon (search "Books")	http://www.amazon.com/
Google Book Search	http://books.google.com/

Live Book Search (Beta)	http://books.live.com/
Metasearch for Books	http://kokogiak.com/booksearch/

The "Invisible Web"

A9	http://www.a9.com/
Aardvark Asian Databases	http://www.aardvarknet.info/user/subject26/index.cfm?all=All
Amazon	http://www.amazon.com/
Answers	http://www.answers.com/
BUBL Catalog	http://www.bubl.ac.uk/link/
The Complete Planet	http://www.completeplanet.com/
Deep Web Research	http://www.deepwebresearch.com/
Infomine	http://infomine.ucr.edu/
Intute (formerly RDN)	http://www.intute.ac.uk/
Pinakes Subject Launchpad	http://www.hw.ac.uk/libWWW/irn/pinakes/pinakes.html
Research Beyond Google: 119 Authoritative, Invisible, and Comprehensive Resources	http://oedb.org/library/college-basics/research-beyond-google
The Wayback Machine	http://web.archive.org/

Scholarly Search

Answers.com	http://www.answers.com/
Citeseer☆	http://citeseer.ist.psu.edu/
CiteULike	http://www.citeulike.org/
Cornell University's arXiv.org	http://arxiv.org/
Foreign Doctoral Dissertations	http://www.crl.edu/content.asp?l1=5&l2=23&l3=44&l4=25
Google Scholar	http://scholar.google.com/
Ingenta Connect	http://www.ingentaconnect.com/
Infomine's Electronic Journals Search	http://infomine.ucr.edu/cgi-bin/search?ejournal
ISI Highly Cited	http://isihighlycited.com/
Live Academic	http://academic.live.com/
OAIster	http://www.oaister.org/

Research Now	http://researchnow.bepress.com/
Scholar Universe	http://www.scholaruniverse.com/index.jsp
Science Direct (select Abstract Databases tab)	http://www.sciencedirect.com/
Scirus	http://www.scirus.com/srsapp/
Wiley InterScience Journal Search	http://www3.interscience.wiley.com/

Browser-Related Pages

Microsoft Internet Explorer	http://www.microsoft.com/windows/ie/default.htm
Mozilla Firefox	http://www.mozilla.com/firefox/
Netscape 7.1 Streamline	http://sillydog.org/narchive/sd/71.html
Netscape Archive (7.1 or 7.2)	http://browser.netscape.com/ns8/download/archive.jsp

Search News and Blogs

Google Operating System	http://googlesystem.blogspot.com/
John Battelle's Searchblog	http://battellemedia.com/
Live Search Weblog	http://blogs.msdn.com/msnsearch/default.aspx
Official Google Blog	http://googleblog.blogspot.com/
Pandia Search Central	http://pandia.com/
Philipp Lenssen's Google Blogoscoped	http://blog.outer-court.com/
Phil Bradley's Weblog	http://philbradley.typepad.com/phil_bradleys_weblog/
Research Buzz	http://www.researchbuzz.com/
Resource Shelf	http://www.resourceshelf.com/
Search Day	http://searchenginewatch.com/searchday/
Search Engine Showdown	http://www.searchengineshowdown.com/
Search Engine Watch	http://searchenginewatch.com/
Search Engine Watch Web Searching Tips	http://www.searchenginewatch.com/facts/index.html
Web Master World	http://www.webmasterworld.com/
Web Search Guide	http://www.websearchguide.ca/
Search Engine Watch Blog	http://blog.searchenginewatch.com/blog/
Yahoo Search Blog	http://www.ysearchblog.com/

Links to Online Dictionaries

Foreignword	http://www.foreignword.com/Tools/dictsrch.htm
Language Automation's Glossaries	http://www.rahul.net/lai/glossaries.html
Martindale's Language and Translation Center	http://www.martindalecenter.com/Language.html
Paderborn University List of Dictionaries	http://www-math.uni-paderborn.de/dictionaries/Dictionaries.html
Word2Word	http://www.word2word.com/dictionary.html
yourDictionary	http://www.yourdictionary.com/

Online Multilingual Dictionaries

Digital Dictionaries of South Asia	http://dsal.uchicago.edu/dictionaries/
Eurodicautom*	http://europa.eu.int/eurodicautom/Controller
Foreignword	http://www.foreignword.com/Tools/dictsrch.htm
Language to Language	http://www.langtolang.com/
Logos *	http://www.logos.it/lang/transl_en.html
OneLook Dictionaries	http://www.onelook.com/
Online Dictionary English↔French, German, Spanish, Italian, Japanese, Chinese, Russian	http://www.online-dictionary.biz/
Papillon Project English↔Estonian, German, French, Japanese, Vietnamese, Korean, Malay, Chinese	http://www.papillon-dictionary.org/Home.po
FreeDict	http://www.freedict.com/
Travlang's Translating Dictionaries	http://dictionaries.travlang.com/
UltraLingua English↔German, French, Spanish, Italian, Portuguese, Esperanto, Latin	http://www.ultralingua.net/
Word Reference	http://www.wordreference.com/

Online Text Translators

AjaxTrans	http://ajax.parish.ath.cx/translator/
Babelfish from Yahoo	http://babelfish.yahoo.com/
FreeTranslation**	http://www.FreeTranslation.com/
Foreignword	http://foreignword.com/Tools/transnow.htm
Google Language Tools	http://www.google.com/language_tools

InterTran**	http://www.tranexp.com/win/itserver.htm
Mezzofanti Translations	http://www.mezzofanti.org/translation/
PhraseBase	http://www.phrasebase.com/english/phrases/
PopJisyo (Asian languages)	http://www.online-dictionary.biz/
PROMT**	http://www.translate.ru/eng/text.asp
Reverso**	http://www.reverso.net/text_translation.asp
VoyCabulary	http://www.voycabulary.com/
WorldLingo**	http://www.worldlingo.com/products_services/worldlingo_translator.html
yourDictionary	http://www.yourdictionary.com/diction1.html#translate

Online Web Page Translators

Ajeeb! Arabic ↔ English+	http://tarjim.ajeeb.com/ajeeb/default.asp?lang=1
Babelfish from Yahoo	http://babelfish.yahoo.com/
Google Language Tools	http://www.google.com/language_tools
InterTran**	http://www.tranexp.com/win/itserver.htm
PROMT	http://www.translate.ru/eng/srvurl.asp
Reverso**	http://www.reverso.net/url_translation.asp
Systran	http://www.systransoft.com/
VoyCabulary	http://www.voycabulary.com/
WorldLingo**	http://www.worldlingo.com/en/websites/url_translator.html

+ Requires free registration
* Translates to/from multiple languages at once
** Site offers virtual keyboard or special characters for non-English translations

Finding International Search Engines

All Search Engines.com	http://www.allsearchengines.com/foreign.html
Beaucoup!	http://www.beaucoup.com/
European Search Engines	http://www.netmasters.co.uk/european_search_engines/
FetchFido European Search Engines	http://homepage.ntlworld.com/fetchfido2/interface/search_engines_european.htm
FetchFido World Search Engines	http://homepage.ntlworld.com/fetchfido2/interface/search_engines_worldwide.htm
FinderSeeker	http://www.finderseeker.com/

Google International Sites	http://www.google.com/language_tools
Infisource Foreign Language Search Engines	http://www.infinisource.com/search-engines.html#foreign
International Search Engines	http://www.arnoldit.com/lists/intlsearch.asp
ISEDB Local and Regional Search Engines	http://www.isedb.com/html/Internet_Search_Engines/Local_and_Regional_Search_Engines/
ISEDB Local and Regional Directories	http://www.isedb.com/html/Web_Directories/Local_and_Regional_Directories/
Phil Bradley's Country Based Search Engines	http://www.philb.com/countryse.htm
Regional and Special Search Engines	http://www.ntu.edu.sg/lib/search/specialframe.htm
Search Engine Colossus★	http://www.searchenginecolossus.com/
Search Engine Guide	http://www.searchengineguide.com/pages/Regional/
Search Engine Index	http://www.search-engine-index.co.uk/Regional_Search/
Search Engines 2	http://www.search-engines-2.com/
Search Engines Worldwide (2003)	http://home.inter.net/takakuwa/search/
Ultimate Search Engines Links Page	http://www.searchenginelinks.co.uk/
Yahoo International	http://world.yahoo.com/

Finding Email Directories

Email-Directory.com	http://www.email-directory.com/
Nedsite	http://www.nedsite.nl/search/people.htm#email

International Email Lookup Tools

Addresses.com	http://www.allemailaddresses.com/
Infospace Email Lookup	http://www.infospace.com/home/white-pages/email-search
Infospace Reverse Email Lookup	http://www.infospace.com/home/white-pages/reverse-email
Look4U	http://www.look4u.com/english/
MESA MetaEmailSearchAgent	http://mesa.rrzn.uni-hannover.de/
Peoplesearch Reverse Email Search	http://peoplesearch.net/peoplesearch/peoplesearch_reverse_email_address.html
World Email Directory	http://www.worldemail.com/freemail.htm

Email Megadirectories

Freeality Email Lookup	http://www.freeality.com/findet.htm
Infospace International Directories	http://www.infospace.com/intl/int.html
MESA MetaEmailSearchAgent	http://mesa.rrzn.uni-hannover.de/
Nedsite	http://www.nedsite.nl/search/people.htm#email
Peoplesearch	http://peoplesearch.net/peoplesearch/peoplesearch_reverse_email_address.html
Infobel Email Lookup	http://www.infobel.com/teldir/teldir.asp?page=/eng/more/email

Tools for International Telephone Lookups

AnyWho International	http://www.anywho.com/international.html
AOL International Directories	http://www.aol.com/netfind/international.html
EscapeArtist Telephone Search Engine	http://www.escapeartist.com/global/telephone.htm
Global Yellow Pages	http://www.globalyp.com/world.htm
Infobel	http://www.infobel.com/World/default.asp
Infobel's Telephone Directories on the Web	http://www.infobel.com/teldir/
Infospace International Directories	http://www.infospace.com/intl/int.html
International White & Yellow Pages	http://www.wayp.com/
Nedsite	http://www.nedsite.nl/search/people.htm#telephone
Phonebook of the World	http://www.phonebookoftheworld.com/
SBN International Yellow Pages	http://www.sbn.com/international/international.asp

Specialty Telephone Lookups

ACR's International Calling Codes by country	http://www.the-acr.com/codes/cntrycd.htm
ACR's International Calling Codes listed numerically	http://www.the-acr.com/codes/cntryno.htm
Americom's International Decoder	http://decoder.americom.com/
International Dialing Codes	http://kropla.com/dialcode.htm
International City Codes	http://www.numberingplans.com/kropla/
World Telephone Numbering Guide	http://www.wtng.info/index.html

Online Video Search

AOL Video Search	http://search.aol.com/aolcom/videohome
BBC Video	http://news.bbc.co.uk/
Blinkx ★	http://www.blinkx.tv/
CBS News Video Search	http://www.cbsnews.com/sections/i_video/main500251.shtml
CNN Video Homepage	http://www.cnn.com/video/
CNN Video Almanac	http://www.cnn.com/resources/video.almanac/
C-SPAN	http://www.c-span.org/
C-SPAN Store	http://www.c-spanstore.org/shop/
Google Video	http://video.google.com/
IFILM	http://www.ifilm.com/
MSN Video	http://video.msn.com/
Pixsy	http://pixsy.com/
Reuters Video	http://today.reuters.com/tv
RocketInfo	http://www.rocketnews.com/ [select the VIDEO tab]
RooTV	http://www.rootv.com/
Searchforvideo	http://www.searchforvideo.com/home/index.html
Searchforvideo IM Service	http://www.searchforvideo.com/misc/im.jsp
Searchforvideo Reel Time Lens	http://www.searchforvideo.com/misc/reel.jsp
Sky News Video	http://www.sky.com/skynews/video
TVEyes	http://tveyes.com/
Yahoo Video Search	http://video.yahoo.com/
Yahoo News Video	http://news.yahoo.com/video
YouTube	http://www.youtube.com/

Podcasting

Blinkx	http://www.blinkx.tv/
Odeo	http://odeo.com/
Podcast Alley	http://www.podcastalley.com/
Podcast.net	http://www.podcast.net/
Podscope	http://www.podscope.com/

Podzinger	http://www.podzinger.com/
Yahoo Podcast Search (Beta)	http://podcasts.yahoo.com/

Podcast Directories

iPodder	http://www.ipodder.org/directory/4/podcasts
Podcast Directory	http://www.podcastdirectory.com/
Podfeed	http://www.podfeed.net/
Podcasting Station	http://www.podcasting-station.com/
Podcast Shuffle	http://www.podcastshuffle.com/

Newsgroups & Mailing Lists

Google Groups	http://groups.google.com/
BoardReader	http://www.boardreader.com/
BoardTracker	http://www.boardtracker.com/
Omgili	http://www.omgili.com/
Yahoo Groups	http://groups.yahoo.com/
Yahoo Member Directory	http://members.yahoo.com/
CataList	http://www.lsoft.com/lists/listref.html
Tile.net	http://www.tile.net/

Weblog Search

Blogdigger	http://www.blogdigger.com/
Blog Search Engine	http://www.blogsearchengine.com/
Blogwise	http://www.blogwise.com/
Bloogz	http://www.bloogz.com/
Clusty Blog Metasearch	http://blogs.clusty.com/
Daypop	http://www.daypop.com/
Feedster	http://www.feedster.com/
Google Blogsearch	http://blogsearch.google.com/
IceRocket	http://blogs.icerocket.com/
Sphere	http://www.sphere.com/
Technorati☆	http://www.technorati.com/

General News Sources

ABYZ Newslinks	http://www.abyznewslinks.com/
Guardian's World News Guide	http://www.guardian.co.uk/worldnewsguide/
HeadlineSpot	http://www.headlinespot.com/
Kiosken	http://www.esperanto.se/kiosk/engindex.html
Metagrid (newspapers & magazines)	http://www.metagrid.com/
NewsCentral (online newspaper links)	http://www.all-links.com/newscentral/
NewsDirectory	http://newsdirectory.com/
Newslink	http://newslink.org/
Online Newspapers	http://www.onlinenewspapers.com//index.htm
RefDesk (My Virtual Newspaper)	http://www.refdesk.com/papmain.html

News Search Services

Google News	http://news.google.com/
Google News Archive	http://news.google.com/archivesearch
HavenWorks	http://havenworks.com/news/search/
JournalismNet	http://www.journalismnet.com/
MSN Newsbot	http://newsbot.msnbc.msn.com/
NewsNow	http://www.newsnow.co.uk/
Pandia Newsfinder	http://www.pandia.com/news/
Topix.net	http://www.topix.net/
Worldnews	http://www.wn.com/
Yahoo News	http://news.yahoo.com/

Technology News on the Web

Newsfactor Network	http://www.newsfactor.com/
TechNews.com	http://www.washingtonpost.com/wp-dyn/technology/
TechWeb	http://www.techweb.com/
The Register	http://theregister.co.uk/
Wired News	http://www.wired.com/
ZDNet News	http://zdnet.com.com/

Telecommunications on the Web

Analysys Telecoms Virtual Library	http://www.analysys.com/vlib
Computer and Communication Entry Page	http://www.cmpcmm.com/cc
Goodman's Bookmarks	http://www.gbmarks.com/
IT Landscape in Nations Around the World	http://www.american.edu/academic.depts/ksb/mogit/country.html
Lido Telecom Web Central	http://www.telecomwebcentral.com/secure/links/
Bandwidth Market Telecom Links	http://www.bandwidthmarket.com/component/option,com_weblinks/Itemid,4/
World Wide Web Telecommunication Center	http://home.planet.nl/~wvhwvh/teletop.htm

Researching PTTs & Telecom Operators Around the World

Country Index for Major PTTs, PTOs, and Major Service Providers	http://home.planet.nl/~wvhwvh/countidx.htm
Goodman's International Telecom Companies	http://www.gbmarks.com/html/international.html
IT Landscape in Nations Around the World	http://www.american.edu/academic.depts/ksb/mogit/country.html
ITU's Global Directory of Regulators (select ***Regulators*** for PTTs)	http://www.itu.int/cgi-bin/htsh/mm/scripts/mm.search
World Wide Web Telecommunication Resource Center	http://home.planet.nl/~wvhwvh/teletop.htm

Radio, Television, and Satellite Broadcasting

Radio Locator	http://www.radio-locator.com/
Radio, TV, and Satellite Links	http://www.liensutiles.org/sat.htm
Live Radio	http://www.live-radio.net/info.shtml
Radio Station World	http://radiostationworld.com/default.asp
Mike's Radio World	http://www.mikesradioworld.com/
vTuner	http://www.vtuner.com/
USC Satellite Database	http://www.ucsusa.org/global_security/space_weapons/satellite_database.html
Heaven's Above Satellite Database	http://www.heavens-above.com/selectsat.asp

SatcoDX Satellite Chart	http://www.satcodx.com/eng/
NASA's J-Track Satellite Tracking	http://science.nasa.gov/RealTime/JTrack/
Small Satellites Home Page	http://centaur.sstl.co.uk/SSHP/

Search for People

Biography Center	http://www.biography-center.com/
Biography Reference Center from MacGill University	http://www.library.mcgill.ca/refshelf/biograph.htm
Chinese Biographical Database	http://www.lcsc.edu/cbiouser/
Wolfram's Science World Biography	http://scienceworld.wolfram.com/biography/
ISI Highly Cited Researchers	http://www.isihighlycited.com/
Google Groups	http://groups.google.com/
Yahoo Member Directory	http://members.yahoo.com/
ICQ User Directory	http://people.icq.com/whitepages/
Forbes People Lists	http://www.forbes.com/lists/
Search the SEC's Edgar Database	http://searchwww.sec.gov/EDGARFSClient/jsp/EDGAR_MainAccess.jsp
SurfWax SEC Search	http://lookahead.surfwax.com/edgar/
EdgarScan Advanced Search	http://edgarscan.pwcglobal.com/servlets/advancedsearch
Deadline Online's People Finders	http://www.deadlineonline.com/peoplefinders.html
Langenberg.com Person Finder	http://person.langenberg.com/
LexNotes Telephone and Email Directories	http://www.lexnotes.com/sources/people/fonemail.shtml
Pandia People Search	http://www.pandia.com/people/
People Search Engines	http://www.people-search-engines.com/
People Search Links	http://www.peoplesearchlinks.com/
People Search Sites	http://www.nettrace.com.au/resource/search/people.html
Power Reporting People Finders	http://powerreporting.com/category/People_finders
Public Record Finder Outside the US	http://www.publicrecordfinder.com/outside_usa.html
Searchbug People Finder	http://www.searchbug.com/peoplefinder/
Search Systems Free Public Records Database	http://www.searchsystems.net

The Virtual Chase People Finder Guide	http://www.virtualchase.com/people/
The Virtual Chase Finding People Guide	http://www.virtualchase.com/topics/people_finder_index.shtml
The Virtual Gumshoe	http://www.virtualgumshoe.com/
ZoomInfo	http://www.zoominfo.com/
Landings Certified Pilots Database	http://www.landings.com/_landings/pages/search/certs-pilot.html
The Virtual Chase Criminal Records	http://www.virtualchase.com/resources/criminal_records.html
CrimeNet	http://www.crimenet.com.au/
The Black Book Online	http://www.crimetime.com/online.htm
NameBase	http://www.namebase.org/

Business Search & Research

10K Wizard	http://www.10kwizard.com/
Annual Reports from Report Gallery	http://www.reportgallery.com/
Arab Data Net	http://www.arabdatanet.com/
Business.com	http://www.business.com/
Business Information on the Internet	http://www.rba.co.uk/sources/index.htm
Corporate Information	http://www.corporateinformation.com/
Search the SEC's Edgar Database	http://www.sec.gov/edgar/searchedgar/webusers.htm
EdgarScan Advanced Search	http://edgarscan.pwcglobal.com/servlets/advancedsearch
Free Reports for Top 20 European Companies	http://amadeus.bvdep.com/amadeus/top20/_top20.htm
Global Edge International Business Research (Michigan State University)	http://globaledge.msu.edu/ibrd/ibrd.asp
Hoovers*	http://www.hoovers.com/
Kompass*	http://www.kompass.com/
MacRae's Blue Book	http://www.macraesbluebook.com/
MacRae's EuroPages Search	http://www.europages.net/co_branding/macraesbluebook/home-en.html
Market Access and Compliance	http://www.mac.doc.gov/

MSN Money's Key Developments	http://news.moneycentral.msn.com/ticker/sigdev.asp
PRNewswire	http://www.prnewswire.com/
Researching Businesses and Non-Profits on the Web	http://www.ojr.org/ojr/technology/1028068074.php
Researching Companies Online	http://www.learnwebskills.com/company/
The Scannery	http://www.thescannery.com/
SEDAR	http://www.sedar.com/
ThomasGlobal★	http://www.thomasglobal.com/
Virtual Business Information Center	http://www.vbic.umd.edu/
Virtual International Business and Economic Sources	http://library.uncc.edu/display/?dept=reference&format=open&page=68
Yahoo Finance Press Releases	http://biz.yahoo.com/prnews/

*Full access requires subscription, but limited information is free.

Researching Countries

Aardvark: Asian Resources for Librarians	http://www.aardvarknet.info/user/aardvarkwelcome/
Academic Info	http://www.academicinfo.net/
Admi.net	http://admi.net/world/
BBC Country Profiles	http://news.bbc.co.uk/1/hi/country_profiles/
BUBL Country List	http://www.bubl.ac.uk/link/countries.html
Bucknell University's Russian Studies	http://www.departments.bucknell.edu/russian/
The Economist Country Briefings	http://www.economist.com/countries/
Google Directory Country Index	http://directory.google.com/Top/Regional/Countries/
Library of Congress Country Studies	http://lcweb2.loc.gov/frd/cs/cshome.html
Middle East and Jewish Studies	http://www.columbia.edu/cu/lweb/indiv/mideast/cuvlm/
NationMaster	http://www.nationmaster.com/
Northwestern University Library Foreign Governments	http://www.library.northwestern.edu/govpub/resource/internat/foreign.html
Northwestern University Library International Governmental Organizations	http://www.library.northwestern.edu/govpub/resource/internat/igo.html
The Organization for Economic Co-operation and Development	http://www.oecd.org/

Unrepresented Nations and Peoples Organization (UNPO)	http://www.unpo.org/
WWW Virtual Library	http://vlib.org/Regional
Yahoo Countries	http://dir.yahoo.com/regional/countries/index.html

Researching Governments, Political Parties, and Politicians

Council of the Baltic Sea States	http://www.cbss.st/
East & Southeast Asia: An Annotated Directory of Internet Resources	http://newton.uor.edu/Departments&Programs/AsianStudiesDept/index.html
European Countries	http://europa.eu/abc/european_countries/index_en.htm
Foreign Government Resources on the Web	http://www.lib.umich.edu/govdocs/foreign.html
Global Edge	http://globaledge.msu.edu/
InterParliamentary Union	http://www.ipu.org/english/home.htm
Northwestern University's Foreign Governments	http://www.library.northwestern.edu/govpub/resource/internat/foreign.html
Northwestern University's International Governmental Organizations	http://www.library.northwestern.edu/govpub/resource/internat/igo.html
Political Resources on the Net	http://www.politicalresources.net/
Political Resources on the Net: Unrepresented People	http://www.politicalresources.net/int6.htm
Political Database of the Americas	http://www.georgetown.edu/pdba
Current Rulers Worldwide	http://www.terra.es/personal2/monolith/
Rulers of the World	http://rulers.org/

Finding Foreign Ministries

Library of Congress: Portals to the World	http://www.loc.gov/rr/international/portals.html
Ministries of Foreign Affairs from Lawresearch	http://www.lawresearch.com/v10/global/ciministries.htm
Stefano Baldi's Ministries of Foreign Affairs Online	http://hostings.diplomacy.edu/baldi/mofa.htm
US Institute of Peace Library Foreign Affairs Ministries on the Web	http://www.usip.org/library/formin.html

Finding Embassies

Embassies & Consulates Worldwide	http://www.mypage.bluewin.ch/caccia/
Embassy.org	http://www.embassy.org/
Embassy World	http://www.embassyworld.com/
Latin American Embassies	http://www-personal.si.umich.edu/~rlwls/embajadas.html
Library of Congress: Portals to the World	http://www.loc.gov/rr/international/portals.html
Tagish Worldwide Embassies	http://www2.tagish.co.uk/Links/embassy1b.nsf/
Yahoo Embassies and Consulates	http://dir.yahoo.com/Government/Embassies_and_Consulates/

Internet Surveys and Statistics

Clickz Stats	http://www.clickz.com/stats/
Cyberatlas	http://cyberatlas.internet.com/
Global Reach's Global Internet Statistics by Language	http://www.glreach.com/globstats/
Internet Traffic Report	http://www.internettrafficreport.com/main.htm
Netcraft	http://news.netcraft.com/
Network Wizards Domain Survey	http://www.isc.org/ds
Zooknic Internet Statistics	http://www.zooknic.com/

ICANN and the Regional Internet Registries (aka NICs)

ICANN	http://www.icann.org
AfriNIC	http://www.afrinic.net/
APNIC	http://www.apnic.net
ARIN	http://www.arin.net
European Registry of Internet Domain Names (EURid)	http://www.eurid.eu/
LACNIC	http://lacnic.net/en
RIPE	http://www.ripe.net

Ipv6

Ipv6 Information Page	http://www.ipv6.org/

Domain Name Resources

Ins and Outs of DNS	http://www.webmonkey.com/webmonkey/02/31/index3a.html
DNS for Rocket Scientists	http://newweb.zytrax.com/books/dns/ch1/
The Domain Name Service	http://www.scit.wlv.ac.uk/~jphb/comms/dns.html
DNS and BIND, 3rd Edition, O'Reilly Online Catalog	http://www.oreilly.com/catalog/dns3/chapter/ch02.html
Domain Name Registries Around the World	http://www.norid.no/domreg.html
IANA's Contact List for TLD Administrators	http://www.iana.org/cctld/cctld-whois.htm
InterNIC FAQ on New Top-level Domains	http://www.internic.net/faqs/new-tlds.html
Whois Data Problem Report System	http://wdprs.internic.net/
Yahoo's Computers and Internet Domain Name Registration	http://dir.yahoo.com/Computers_and_Internet/Internet/Domain_Name_Registration/→ Top_Level_Domains__TLDs_/Registry_Operators/International_Country_Codes/

NSLookup Tools

AnalogX	http://www.analogx.com/contents/dnsdig.htm
Check DNS	http://www.checkdns.net/quickcheck.aspx
DNS Stuff*	http://www.dnsstuff.com/
Eye-Net Consulting*	http://www.enc.com.au/itools/
Infobear	http://www.infobear.com/nslookup.shtml
Multiple NSLookup	http://www.bankes.com/nslookup.htm
SmartWhois NSLookup	http://swhois.net/
Squish DNS Lookup	http://www.squish.net/dnscheck/
WebReference NsLookup Gateway	http://www.webreference.com/cgi-bin/nslookup.cgi
ZoneEdit NSLookup	http://www.zoneedit.com/lookup.html?ad=goto&kw=nslookup

*These sites provide Ipv6 lookups in addition to Ipv4.

Whois Queries

APNIC Whois lookups	http://www.apnic.net/search/index.html
APNIC Whois help	http://www.apnic.net/db/search/all-options.html
ARIN	http://www.arin.net/whois/index.html

ARIN Whois help	http://www.arin.net/tools/whois_help.html
AfriNIC Whois	http://www.afrinic.net/cgi-bin/whois
AfriNIC User Manual	http://www.afrinic.net/docs/db/afsup-dbgs200501.htm
EURid Whois	http://www.whois.eu/whois/GetDomainStatus.htm
LACNIC Whois	http://lacnic.net/cgi-bin/lacnic/whois
RIPE	http://www.ripe.net/perl/whois/
RIPE Reference Manual	http://www.ripe.net/ripe/docs/databaseref-manual.html
RIPE Whois help	http://www.ripe.net/ripencc/pub-services/db/whois/whoishelp.html

Domain Queries

Allwhois	http://www.allwhois.com/
CheckDNS☆	http://www.checkdns.net/quickcheck.aspx
Checkdomains	http://www.checkdomain.com/
CoolWhois	http://www.coolwhois.com/
DNS411	http://dns411.com/
Domain Dossier	http://centralops.net/co/DomainDossier.vbs.asp
Domainsearch	http://www.domainsearch.com/
Domainsurfer	http://www.domainsurfer.com/
Domain Tools	http://www.domaintools.com/
Domain Tools Whois Source	http://whois.domaintools.com/
DrWhois	http://www.drwhois.com/
EasyWhois	http://www.easywhois.com/
Geektools	http://www.geektools.com/whois.php
IP-Plus	http://www.ip-plus.ch/tools/whois_set.en.html
MSV.DK Network Whois	http://msv.dk/ms593.aspx
Multiple DNS Lookup Engine	http://www.bankes.com/nslookup.htm
Namedroppers	http://www.namedroppers.com/
Netcraft	http://news.netcraft.com/
Network-Tools	http://network-tools.com/
Whois.net	http://www.whois.net/
Whois at Webhosting.info	http://whois.webhosting.info/
Whoix?	http://www.whoix.com/

Whoix? Advanced Search	http://www.whoix.com/advdomsearch.html
Xwhois	http://www.xwhois.com/

Internet Utilities and Tools for Windows

All-Nettools.com	http://www.all-nettools.com/tools1.htm
Centralops	http://centralops.net/co/body.asp
Domtools.com	http://www.domtools.com/domtools/
Internet Query Tools	http://www.demon.net/external/
iTools Internet Tools	http://www.itools.com/internet/
Logbud Online Tools★	http://www.logbud.com/
Network-Tools	http://www.network-tools.com/
RodentNet Ad Hoc IP Tools	http://tatumweb.com/iptools.htm

Traceroute Tutorials

Mapping Where the Data Flows	http://www.isoc.org/oti/articles/0200/dodge.html
Traceroute Tutorial	http://www.exit109.com/~jeremy/news/providers/traceroute.html
Russ Haynal's Traceroute Overview	http://navigators.com/traceroute.html

Traceroute for Windows

All Nettools.com	http://www.all-nettools.com/toolbox
Cogentco	http://www.cogentco.com/htdocs/glass.php
Geektools Traceroute	http://www.geektools.com/traceroute.php
IP-Plus Traceroute Servers	http://www.ip-plus.ch/tools/traceroute.en.html
Logbud Online Tools★	http://www.logbud.com/
Multiple Traceroute Gateway	http://www.tracert.com/cgi-bin/trace.pl
New York Internet Traceroute Links	http://www.nyi.net/traceroute.html
Opus One Traceroute	http://www.opus1.com/www/traceroute.html
SixXs IPv4 and IPv6 Traceroute	http://www.sixxs.net/tools/traceroute/
Traceroute.org	http://www.traceroute.org/
Tracerouters Around the World	http://tracerouters.nielssen.com/
BGPNet IPv4 Wiki	http://www.bgp4.net/tr

BGPNet IPv6 Wiki	http://www.bgp4.net/tr6

More Traceroute Tools

Airport & City Code Database	http://www.airportcitycodes.com/aaa/CCDBFrame.html
World Airport Codes	http://www.world-airport-codes.com/
Airlines of the Web Airport Codes	http://flyaow.com/airportcode.htm
Sarangworld Traceroute Project Known Hostname Codes	http://www.sarangworld.com/TRACEROUTE/showdb-2.php3

IP Geolocation Tools

DNS Stuff's Version of IP2Location	http://www.dnsstuff.com/
Geobytes' IP Locator	http://www.geobytes.com/IpLocator.htm
GeoIP	http://www.maxmind.com/app/lookup
HuntIP	http://www.huntip.com/Tools/mapips.php
IP2Location	http://www.location.com.my/free.asp
IPAddressGuide.com	http://www.internetipaddress.com/ip2location.aspx
NetGeo	http://www.caida.org/tools/utilities/netgeo/
NetWorldMap's Geolocation Tool	http://www.networldmap.com/TryIt.htm
WebHosting.Info	http://ip-to-country.webhosting.info/node/view/36

Finding ISPs and Email Providers Around the World

The List	http://thelist.internet.com/countrycode.html
NSRC's Connectivity Providers Database	http://www.nsrc.org/networkstatus.html
International Internet Access Providers	http://www.herbison.com/herbison/iap_international_meta_list.html
FreedomList	http://www.freedomlist.com/find.php3
African Internet Connectivity	http://www3.sn.apc.org/africa/af-isps.htm

Middle East Directory List of ISPs http://www.middleeastdirectory.com/me-isps.htm

Satellite Internet Service Providers for North & South America, Europe, Africa, Asia, Middle East http://www.satsig.net/

Linksat Satellite and Internet Providers http://www.linksat.com/

Satellite Industry Links: Satellite Service Providers http://www.satellite-links.co.uk/links/ssp.html

ISP Directories

Google Directory http://directory.google.com/Top/Computers/Internet/Access_Providers/

Yahoo http://dir.yahoo.com/

There are several ways to use Yahoo to find international ISPs. The best is: Business_and_Economy→Business_to_Business→Communications_and_Networking→Internet_and_World_Wide_Web→By_Region

WiFi Hotspot Finders

Hotspothaven http://www.hotspothaven.com/

Intel's Mobile Technology Hotspot Finder http://intel.jiwire.com/

iPass Hotspot Finder http://ipass.jiwire.com/

JiWire Global WiFi Hotspot Finder http://www.jiwire.com/search-hotspot-locations.htm

WiFinder http://www.wifinder.com/

WiFi411 http://www.wifi411.com/

Wi-Fi Hotspot List http://www.wi-fihotspotlist.com/

Cybercafe Finders

Curious Cat Cybercafe Connections http://www.curiouscat.com/travel/cybercafe.cfm

Cybercaptive Search Engine http://cybercaptive.com/

The country search is disabled; search by city

Google Directory: Cybercafes http://directory.google.com/Top/Computers/Internet/Cybercafes/

Indra's International Cybercafes http://www.indranet.com/potpourri/links/cybercafeint.html

Internet Cybercafe Database http://cybercafe.katchup.co.nz/search.asp

Netcafe Guide http://www.world66.com/netcafeguide

Internet Exchanges and Backbone Networks

Colosource Internet eXchange Points	http://www.colosource.com/ix.asp
Exchange Point Information	http://www.ep.net/ep-main.html
Boardwatch's Internet Backbone Maps	http://www.nthelp.com/maps.htm
BT Infonet's Network Maps	http://www.bt.infonet.com/services/internet/network_maps.asp
BWM's Links to Network Maps	http://www.bandwidthmarket.com/component/option,com_weblinks/catid,74/Itemid,4/
Russ Haynal's Major Internet Backbones	http://www.navigators.com/isp.html

Check Your Internet Profile and Vulnerability

Shields Up!	http://www.grc.com/
Junkbusters	http://www.junkbusters.com/cgi-bin/privacy
BrowserHawk Browser Analysis	http://www.syscape.com/showbrow.aspx
Browser Spy Browser Analysis	http://gemal.dk/browserspy/
Russ Haynal's Persona Check	http://navigators.com/cgi-bin/navigators/persona.pl
HackerWhacker Free Tools	http://whacker4.hackerwhacker.com/freetools.php especially the Browser Leakage and Quick Scan for open ports
Sygate/Symantec Online Security Services	http://scan.sygate.com/home_homeoffice/sygate/index.jsp

Improving Your General Computer & Network Security

About's Network Security	http://netsecurity.about.com/
CERT's Home Network Security	http://www.cert.org/tech_tips/home_networks.html
Get Safe Online	http://www.getsafeonline.org/
Microsoft Security & Privacy for Home Users	http://www.microsoft.com/athome/security/default.mspx
NSA's Security Recommendation Guides	http://www.nsa.gov/snac/
NCSA's Stay Safe Online	http://www.staysafeonline.info/
Surf the Net Safely	http://surfthenetsafely.com/
SecureMac.com	http://www.securemac.com/

Securing Home Computers and Networks

Tweakhound's Securing Windows XP
http://www.tweakhound.com/xp/security/page_1.htm

Fred Langa's 5 Essential Steps To PC Security
http://www.informationweek.com/shared/printableArticle.jhtml?articleID=177100010

NIST's Guidance for Securing Windows XP Home Edition
http://csrc.nist.gov/itsec/guidance_WinXP_Home.html

CERT's Home Network Security http://www.cert.org/tech_tips/home_networks.html

Gary Kessler's Protecting Home Computers and Networks
http://www.garykessler.net/library/protecting_home_systems.html

University of Cambridge's Securing Windows XP Home Edition for Stand Alone Use
http://www-tus.csx.cam.ac.uk/pc_support/WinXP/collegehome.html

Lawrence Berkeley Lab's Checklist for Securing Windows XP **PRO**
http://www.lbl.gov/ITSD/Security/systems/wxp-security-checklist.html

Windows XP Security Checklist
http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm

Tom-Cat.com's Secure Your Home Computer v.2.22
http://www.tom-cat.com/security.html

Browser Setup & Testing

ScanIt's Browser Security Check http://www.scanit.be/bcheck

Microsoft Security Home Page http://www.microsoft.com/security/

Microsoft Internet Explorer Security Updates
http://www.microsoft.com/windows/ie/downloads/default.asp

Microsoft Office Download Center http://office.microsoft.com/downloads/

Microsoft Windows Update Page http://update.microsoft.com/windowsupdate/

Microsoft IE7: Dynamic Security Protection
http://www.microsoft.com/windows/products/winfamily/ie/features.mspx

Microsoft: Improve the Safety of Your Browsing and E-Mail Activities
http://www.microsoft.com/athome/security/online/browsing_safety.mspx

How to surf more safely with Internet Explorer 7
http://www.helpwithwindows.com/techfiles/ie7-surf-safe.html

Marc Liron, Microsoft MVP on Internet Explorer 7
http://www.updatexp.com/internet-explorer-7-download.html

Brian Livingston, Windows Secrets, IE7 Needs Tweaking for Safety
http://windowssecrets.com/comp/061026/ - story1

Diana Huggins, IE 7.0's Internet Options Privacy and Security Settings
http://www.lockergnome.com/nexus/windows/2007/01/22/ie-70s-internet-options-security-settings/
http://www.lockergnome.com/nexus/windows/2007/01/23/ie-70s-internet-options-privacy-settings-part-i/
Be sure to look at Part II as well.

Deb Shinder, Tech Republic, "10 things you should know about Internet Explorer 7 Security" http://articles.techrepublic.com.com/5100-1009_11-6130844.html

Surf the Web Safely: Make IE7 Safer http://surfthenetsafely.com/ieseczone8.htm

Kim Komando's Firefox 2 and IE7's Security Settings
http://www.komando.com/tips/index.aspx?id=2523

Cookies

Firefox's Cookie Options
http://mozilla.gunnars.net/firefox_help_firefox_cookie_tutorial.html

Microsoft's Help Safeguard Your Privacy on the Web (for IE6, but most still applies to IE7) http://www.microsoft.com/windows/ie/using/howto/privacy/config.mspx

Cookie Central's Reviews of Cookie Management Software
http://www.cookiecentral.com/files.htm

Junkbusters Cookie Page http://www.junkbusters.com/ht/en/cookies.html

Microsoft Security

Microsoft Internet Explorer Security Updates
http://www.microsoft.com/windows/ie/downloads/default.asp

Microsoft Office Download Center http://office.microsoft.com/downloads/

All Microsoft Office Viewers http://www.microsoft.com/office/000/viewers.asp

Microsoft Policies on Software Distribution
http://www.microsoft.com/technet/security/topics/policy/swdist.mspx

Microsoft Security Home Page http://www.microsoft.com/security/

Microsoft Windows Update Page http://windowsupdate.microsoft.com/

5 Steps to Secure Windows XP Home
http://netsecurity.about.com/cs/windowsxp/a/aa042204_2.htm

Non-Admin Blog, Aaron Margosis' Weblog
http://blogs.msdn.com/aaron_margosis/archive/2005/04/18/TableOfContents.aspx

"RunAs" basic (and intermediate) topics, Aaron Margosis' Weblog
http://blogs.msdn.com/aaron_margosis/archive/2004/06/23/163229.aspx

Email Security

About.com Email Help Center	http://antivirus.about.com/library/bloutlook.htm
About's Email Wiretapping Article	http://antivirus.about.com/library/weekly/aa020501a.htm?once=true&
How Spammers Get Your Email Address	http://www.junk-mail.org.uk/public/articles/spam.html
A Quick Guide to Email Security	http://www.zzee.com/enh/email_security.html
Security Focus: "Securing Privacy: E-mail Issues"	http://www.securityfocus.com/infocus/1579

Anti-Phishing

How Not to Get Hooked by a "Phishing" Scam	http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm
The Anti-Phishing Working Group	http://www.antiphishing.org/
Phishtank (known and suspected phishing sites)	http://www.phishtank.com/
PayPal's Protect Yourself from Fraudulent Emails	https://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/SecuritySpoof-outside
URL Decrypter	http://www.cyber-junkie.com/tools/urldecrypter.shtml
Un-Obfuscating URLs	http://www.wilsonmar.com/1tcpaddr.htm

Disabling Visual Basic Script

How to Disable VBS	http://www.cvm.uiuc.edu/net/virus/outlook.html
Disable Windows Scripting Host	http://www.sophos.com/support/faqs/wsh.html
Remove Windows Scripting Host	http://www.f-secure.com/virus-info/u-vbs/

See What Your Computer is Loading and Running

Greatis Start Up Application Database	http://www.greatis.com/regrun3appdatabase.htm
Pacman's Start-Up Applications	http://www.pacs-portal.co.uk/startup_index.htm
or	http://www.sysinfo.org/startupinfo.html
Process ID	http://www.processid.com/
Answers That Work	http://www.answersthatwork.com/Tasklist_pages/tasklist.htm
Process Library	http://www.processlibrary.com/
PC Hell	http://www.pchell.com/

Encrypt Data in Windows XP

How to Encrypt a File in Windows XP http://support.microsoft.com/kb/307877

How to Encrypt a Folder in Windows XP http://support.microsoft.com/kb/308989

Anti-Virus Information

About's Free Antivirus Software Reviews
http://antivirus.about.com/od/freeantivirussoftware/Free_Antivirus_Software.htm

VirusList Virus Encyclopedia http://www.viruslist.com/en/viruses/encyclopedia

Spyware Checkers and Information

Free Antispyware Products

Ad-Aware Spyware Checker
http://www.lavasoftusa.com/products/ad-aware_se_personal.php

Windows Defender
http://www.microsoft.com/athome/security/spyware/software/default.mspx

Spybot Search & Destroy http://www.safer-networking.org/en/home/index.html

Antispyware Guides & Articles

11 Signs of Spyware
http://www.pcmag.com/article2/0%2C1759%2C1522648%2C00.asp

Anti-Spyware Guide http://www.firewallguide.com/spyware.htm

Monitoring Software on Your Computer: Spyware, Adware, and Other Software, Staff Report, Federal Trade Commission, March 2005 **[PDF]**
http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

PC Hell Spyware Removal Help http://www.pchell.com/support/spyware.shtml

Spychecker http://www.spychecker.com/

Spyware Guide http://www.spywareguide.com/product_list_full.php

Spyware Warrior Rogue/Suspect Anti-Spyware Products
http://www.spywarewarrior.com/rogue_anti-spyware.htm

Spyware Watch http://www.spyware.co.uk/

Stop Internet Abuse http://www.celticsurf.net/webscape/abuse.html

Web Bugs

Bugnosis	http://www.bugnosis.org/
Web Bug FAQ	http://www.bugnosis.org/faq.html
Guidescope	http://www.guidescope.com/home/
WebWasher[235]	http://www.cyberguard.com/products/webwasher/webwasher_products/classic/index.html

Trojan Horse Prevention, Detection, and Removal

List of Trojan Ports	http://secured.orcon.net.nz/portlist_list.html
Onctek's Trojan Port List	http://www.onctek.com/trojanports.html
Anti-Trojan Software Reviews	http://www.anti-trojan-software-reviews.com/
Anti-Trojan.org	http://www.anti-trojan.org/
Anti-Trojan Guide from Firewall Guide	http://www.firewallguide.com/anti-trojan.htm
PCFlank's Trojan Test Page	http://www.pcflank.com/trojans_test1.htm
WindowSecurity.com TrojanScan	http://www.windowsecurity.com/trojanscan/

Passwords

The Simplest Security: A Guide To Better Password Practices	http://www.securityfocus.com/infocus/1537
Microsoft: How to Create Stronger Passwords	http://www.microsoft.com/security/articles/password.asp
Password Security Guide	http://www.umich.edu/~policies/pw-security.html
Fred Langa: How to Build Better Passwords	http://www.informationweek.com/story/showArticle.jhtml?articleID=164303537

Firewall Information

Firewallguide's Personal Firewall Review	http://www.firewallguide.com/software.htm
Firewallguide: Wired Routers	http://www.firewallguide.com/hardware.htm
Firewall Forensics	http://www.linuxsecurity.com/resource_files/firewalls/firewall-seen.html

[235] "Cyberguard has changed the license for Webwasher Classic to Donationware and asks you to make a donation before downloading Webwasher Classic." However, the donation is voluntary.

Firewall Q&A	http://www.vicomsoft.com/knowledge/reference/firewalls1.html
Free Personal Firewall Software	http://netsecurity.about.com/od/personalfirewalls/a/aafreefirewall.htm
Gibson Research's Firewall Page	http://grc.com/su-firewalls.htm
HomeNetHelp's Broadband Router Guide	http://www.homenethelp.com/router-guide/index.asp
How Firewalls Work	http://www.howstuffworks.com/firewall.htm
Internet Firewall FAQ	http://www.interhack.net/pubs/fwfaq/
Introduction to Firewalls	http://netsecurity.about.com/od/hackertools/a/aa072004.htm

Free Software Firewalls for Windows

Securepoint	http://www.securepoint.cc/products_pcfirewall_en.html
Sygate Personal Firewall	http://smb.sygate.com/products/spf_standard.htm
Zone Alarm	http://www.zonelabs.com/

Firewall Leak Tests

Gibson Research's Firewall Leaktest	http://grc.com/lt/leaktest.htm
PCFlank Firewall Leaktest	http://www.pcflank.com/pcflankleaktest.htm
Tooleaky	http://tooleaky.zensoft.com/
Firehole	http://keir.net/firehole.html
Firewall Leak Tester (Test Results)	http://www.firewallleaktester.com/index.html

Anonymizing Proxies

InfoAnarchy's Anonymous Web Searching	http://www.infoanarchy.org/en/Anonymous_Web_Surfing
Free Web Anonymizer Services	http://www.cexx.org/anony.htm
Web Anonymizing Services	http://www.computerbytesman.com/anon/index.htm
Test Page for Web Anonymizing Services	http://www.computerbytesman.com/anon/test.htm

Internet Security and Privacy News and Information

Center for Privacy and Technology Ten Ways to Protect Privacy Online	http://www.cdt.org/privacy/guide/basic/topten.html

EPIC Online Guide to Privacy Resources	http://www.epic.org/privacy/privacy_resources_faq.html
Georgi Guninski Security Research	http://www.guninski.com/
Security Focus	http://www.securityfocus.com/
Security Now!	http://www.grc.com/securitynow.htm
Yahoo News Computer Security	http://fullcoverage.yahoo.com/fc/Tech/Computer_Security
Yahoo News Cybercrime and Internet Fraud	http://news.yahoo.com/fc/Tech/Cybercrime_and_Internet_Fraud/
Yahoo News Internet Privacy	http://news.yahoo.com/fc/Tech/Internet_Privacy/

Notes

Notes

Notes

31228