

INTERNET PRIVACY FOR THE SMALL OR HOME OFFICE ENVIRONMENT

Roland Grefer

Global Support Services Group, Inc.

Jill R. Sommer

Sommer Translation & Net Services

Abstract: Internet privacy for the home and small office is of vital importance to all translators. Many of us work with sensitive and confidential texts, and we need to be aware of the risks involved with the tools we use to communicate with clients and colleagues. There are so many ways that our privacy can be violated—from viruses and spam to breaches in our home and office networks. With our help, you should be able to render your computer, company workstation, home network, or small business network “hack-resistant.” By “hack-resistant,” we do not mean making your system impenetrable, because nothing can do that. However, if you are aware of the risks you will be able to use common sense and layers of protection, also known as defense-in-depth, to make compromising your system more trouble than its worth.

While privacy has been an issue since the dawn of time, the advent of the Internet has made the matter all the more pressing. Surfing the Net can be fun and educational. E-mail is a great way to stay in touch with family and friends, and chat and discussion groups allow you to communicate with people who have similar interests. Most people are aware of the Internet's benefits, but not everyone is aware of how the Internet can threaten personal privacy and the steps you can take to protect your privacy in cyberspace. If you are aware of the dangers involved with Internet use and have taken steps to avoid those dangers, you can surf in peace, knowing that you did your best to be protected.

1. THE BASICS

To protect your computer, your intellectual property, and your clients’ confidentiality, you should at a minimum have the following installed on your computer:

- Antivirus software
 - “Never run your computer without it” is probably sound advice, except in very few, controlled situations. Which anti-virus software you use will in part depend on your specific needs, as well as your budget. No matter which anti-virus software you plan to use, make sure that it updates its signatures automatically. Some “free” anti-virus software (a misinterpretation of the term “non-commercial use”) requires you to download and install updates manually; something you usually won’t take the time to do on a frequent basis (at least once a day).
- A personal firewall
 - This is a software that acts as a filter between your computer and the Internet (or a local area network [LAN] that your computer is connected to). Typically there is no need for the Internet to contact your computer, but rather your computer only needs to contact the Internet. You might have seen these annoying pop-up messages (i.e., when you are connected to one of the cheaper dial-up Internet

service providers) urging you to buy this or that. A personal firewall helps to keep these annoyances out. In addition, it will alert you to unusual behavior of your computer, i.e., caused by infection with a new virus that attempts to "call home."

2. "ALWAYS-ON"

In this day and age, where speed is of the essence, more and more of us are switching from traditional dial-up connections (using an analog modem connected to a phone jack) to the much faster cable modem (connected to your TV cable) or digital subscriber line (DSL, split off of your phone line). In either case, a lot of attacks from the Internet can already be blocked off by plugging an additional piece of hardware in between your computer and the Internet connection like a DSL/cable-modem router. These devices come with a built-in hardware firewall that by default blocks all attempts to connect *to* your computer from the Internet; by default, it lets all connection attempts *from* your computer to the Internet through. An additional benefit of most such devices is that they also allow you to share your high speed Internet connection between multiple computers. In general, you have two options:

- Regular (wired) networking
 - Traditional networking with Ethernet cables allows for the most assurance that nobody is eavesdropping locally on your network, sniffing out your passwords, account numbers, identifications, and other sensitive or confidential information in transit. Please be aware that any information you transmit over the Internet via un-encrypted communication (i.e., to a web or file transfer protocol (FTP) server, or via e-mail) can be spied on, too.
- Wireless networking (WLAN – wireless local area network)
 - In terms of convenience, wireless networking is hard to beat, *but* in order to protect the confidentiality and privacy of communication, it is important to follow some basic advice:
 - Do not use the older technology called 802.11b with a maximum bandwidth of 11 Mbit/s (mega bits per second). Its wireless equivalency protocol (WEP) encryption technology is not sufficiently secure and can easily be cracked by anybody in the vicinity of your home or office (remember, you are no longer on your own little network, but rather are open to the rest of the world).
 - Use newer technology called 802.11g and configure it to only allow connections encrypted via wireless protected access (WPA). This encryption method is much more advanced than WEP and therefore would take an attacker much longer to crack.
 - Do *not* allow 802.11b connections or WEP connections.
 - Change your wireless network's default system identifier (SID); this is the name under which your wireless network advertises itself to any receiver in its proximity. If you leave it at its default name, you typically reveal the manufacturer of your wireless access point, thereby making it much easier for an attacker to determine if there is a vendor-specific vulnerability that could be exploited.
 - Last, but not least, change the default administrator password for your network device. This is something so obvious that it is puzzling why a lot of small office/home office (SOHO) devices are still accessible using default passwords.

3. ELECTRONIC MAIL

How many of us are bombarded with unsolicited commercial e-mail (a.k.a. spam) on a regular basis? How often have you switched e-mail addresses to escape the flood of spam? The amount of unsolicited junk e-mail you receive as a result of your surfing can be an annoyance, but this "spam" is only the most obvious privacy problem. Any e-mail message you send or receive can be intercepted along the way and read – even changed – by anyone from your Internet service provider to the police. It is also easy to retrieve deleted e-mail messages from your computer hard disk or someone else's if you know how. Also, it is possible for other people to send messages under your name, expressing opinions or ordering items without your knowledge, and leaving you to deal with whatever problems that may arise.

What you can do:

- Spam
 - If you receive spam messages, *don't* answer them.
 - Many junk e-mail messages offer the opportunity to remove ("unsubscribe") you from their list. Don't do it! By responding, you confirm your e-mail address is good, and whoever sent you the junk e-mail can sell that address to even more advertisers.
 - Install a spam filter (software) on your computer, then configure your Internet service provider's (ISP) junk filters to allow everything through, thereby allowing you to separate the chaff from the wheat without risking to lose any important messages due to accidental junk-filtering performed by the ISP. Initially you will have to spend a bit of time fine-tuning the out-of-the-box filters of the software, but ultimately you will have a very powerful tool that has been adjusted to your specific needs.
 - Configure your personal firewall software to allow your e-mail program to only communicate on the ports for Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3 - 110/tcp), and Internet Message Access Protocol (IMAP - 143/tcp). These are used by your e-mail program to talk to your ISP's mail server. Spam can contain so called web bugs, tiny graphics sized 1x1 pixel, as well as normal sized graphics which alert the sender that the spam recipient actually exists and was not just an arbitrarily generated new or outdated old address. The only drawback is that you will no longer be able to see graphics that are only included as a link from the Internet, rather than being included in the e-mail itself.
 - While it is tempting to ask your Internet service provider to have junk e-mail deleted before it gets to your mailbox, this bears the risk of the automatism accidentally deleting an important message from an existing or prospective new client.
- Encryption
 - Think of any e-mail as a postcard (an unsealed message that others can read or pass on to someone else). If you want to communicate privately, install software that allows you to "encrypt" or scramble your e-mail messages so no one can read them except you and the person to whom you are writing. Be aware that the recipient in this case also must have the capability to decrypt (unscramble) the e-mail message.

- "Signed" e-mail
 - To assure that e-mail you are sending can not been tampered with, you can electronically sign it with your personal key. This "key" typically is actually a key pair: a private key that only you know and which you should not reveal to anybody as well as a public key which you publish to a public key server. The recipient's e-mail program then connects to the/a public key server to check whether the e-mail that allegedly was sent by you was signed using your key.
- Anonymous re-mailers
 - Even though there are various anonymous re-mailers (organizations that remove your identity from messages before sending them on to their destination) available, be aware that such originating addresses are increasingly blocked by companies and service providers due to the spam problem.
- Recipient control
 - One of the more recent fads is to use e-mail software that lets you control who can see the messages you send – and for how long. Be aware that such products employ the same mechanisms as spam does, and that they are easily circumvented using the aforementioned methods.

4. SURFING THE NET

Many Web sites collect personal information. Some sites ask you to register before you can view the site, while other sites collect information in more subtle ways. Some search engines remember what you have looked for by keeping track of the key words you input. Many other sites store "cookies" (small text files that can collect and store information) on your hard drive to tell them information such as which banner ads you have clicked on, what web sites you have visited, and any information you may have voluntarily provided (like your name, address, etc.). This information allows Web sites to identify you the next time you visit and track your visits. Some cookies are helpful; for instance, Amazon greets you by name every time you visit and keeps track of what you order until you place the order. This is especially helpful if your computer or browser crashes in the middle of an order, because you will not have to go through the process again and try to remember everything you ordered.

Some cookies, however, are not so helpful and enable Web sites or advertising networks to create a profile of you based on the information you provided and your browsing and shopping patterns, often for advertising purposes. Those companies in particular are also commonly employing JavaScript or Dynamic Hyper Text Markup Language (DHTML) to obtain additional information such as your computer's network address and your operating system.

Adware and spyware applications are tiny Trojan horses that are built into other applications that track your habits and violate your privacy without your knowledge. Adware is considered any software application that displays advertising banners while the program is running. For example, a free version of Eudora that we use displays ads while you read your mail. Adware is pretty innocuous. It tracks which ads you have already seen. The real problem lies in spyware. Spyware is software that tracks your online habits and sends that data back to a third party (often without your permission or knowledge). Some companies quietly include spyware as part of the software they sell. In fact, several well-known freeware programs such as Real Audio have been found to include spyware.

What you can do:

- Refuse the cookies that Web sites send you. However, we find this method a bit too Draconian, so we have set our preferences to reject only "third party cookies." Check your browser's Help files to find out how to program your computer to do this. Just remember that some Web sites can make it difficult or even impossible for you to visit them if you do not accept their cookies. In the long run, you must decide whether or not it is worth your while to accept cookies.
- Be cautious about the information you provide to Web sites, because they may use the information for marketing purposes. We have free Web-based accounts like Yahoo set up that we use when ordering online or whenever we are asked for our e-mail address. We only give out our primary e-mail to clients, colleagues, and friends. As a result, we only get very few spam messages a day at our primary addresses and can sometimes go days without getting "spammed."
- Reduce the amount of personal information that you provide to Web sites. Do not provide information that is not required. Also, some financial institutions are now offering one-time credit card numbers for Web purchases to offer greater security. Contact your bank to see if it offers this.
- Before you buy anything or make a financial transaction online, read the Web site's privacy policy. If it does not have one, think twice about completing the transaction. Check opt-out boxes that limit the use of any information you provide. We also go a step further and write "do not pass on or sell my information to third parties" on any warranty or application we fill out in the "real world."

5. CHAT, DISCUSSION, AND NEWS GROUPS

Discussion and news groups are wonderful resources, but you need to remember that anything you write could be used against you. This was illustrated a while ago in a discussion on the German Language Division mailing list. During the course of a discussion, one member made unfounded claims about ATA graders. The behavior then escalated to attacking fellow list members and led to the eventual expulsion of this person from the list. Think before you write.

As just about everyone knows, chat rooms are usually anonymous, and you can be whomever you choose to be in a chat room – as the numerous cases against pedophiles have shown. Newsgroups are in the middle of the spectrum. Participants may be who they say they are; however, they could be misrepresenting themselves as well. Caution is to be exercised in any case. If you take part in discussion and news groups, anyone from the simply curious to potential employers can search for copies of your messages through Google, which archives messages indefinitely. It is also possible to find the names of chat or discussion groups in which you participate and the names of news groups to which you subscribe. The names of those groups alone can reveal a lot about you. Again, a dummy e-mail address can help shield you from this kind of exposure (not to mention from spammers, who use robots to cull discussion groups for e-mails).

What you can do:

- Participate in chat or discussion groups under a fake name or using a web-based e-mail address (please note that you should use your real name in professional discussion groups such as the ATA listservs).

- Be discreet. As a general rule, assume that your online communications are not private unless they are encrypted.
- Some groups that store your old messages allow you to delete them for good: consider it!

6. ADDITIONAL RESOURCES

There are several excellent resources available to help you protect your privacy on the Internet. One excellent book is *Internet Privacy for Dummies* by John Levine, Ray Everett-Church, Gregg Stebben, and David Lawrence. This book can be an eye-opener and covers a wide range of topics from the subjects covered here to telemarketers and Do-Not-Call lists, cell phone usage, etc. You can also visit the web site at <http://www.internetprivacyfordummies.com/>.

There are also a handful of programs (some of them free) that can protect you from peeping businesses and secret software.

Anti-virus products such as Norton AntiVirus (www.symantec.com), McAfee AntiVirus (www.mcafee.com), Kaspersky AntiViral Toolkit Pro (AVP) (www.kaspersky.com), to name but a few help to protect your computer from viruses, worms, and similar malware. While the aforementioned products will be within your budget for installation on a single computer, if you are running up to 10 computers at your office and want to protect them all, you might be better off with F-Prot (www.f-prot.com/products/corporate_users/win/) due to its corporate licensing model (you get 10 licenses for the same price you usually spend on a single license for the others).

Firewalls such as Norton Personal Firewall (www.symantec.com) and Zone Alarm (www.zonealarm.com) shield your computer from prying eyes. If you opt for the corresponding McAfee Personal Firewall product, make sure you obtain their "real" firewall product and not just the McAfee.com Personal Firewall, which only interfaces between your web browser and the Internet, whereas the other personal firewall products protect communication between the Internet and all your applications.

While spyware/adware detectors such as SpyBot Search & Destroy (www.safer-networking.org), Ad-aware (www.lavasoftusa.com), SpyBlocker (personal.bellsouth.net/mia/k/r/kryp), Guidescope (www.guidescope.com), SpyChecker (www.spychecker.com) or Pest Patrol (which is an add-on to Zone Alarm) clean computers of spyware and regulate to some extent what information is gathered by a website, carefully research the spyware detector/blocker you choose to install because some spyware blockers actually contain themselves spyware or adware. The authors have practical experience with SpyBot Search & Destroy and Ad-aware, and, to the best of their knowledge, these two products are benign.

If you would like to look into data encryption and/or electronic signatures, you could explore your e-mail application's built-in digital-ID features or employ a third party product such as the commercial version of Pretty Good Privacy (PGP) (www.pgp.com) or one of the free PGP versions (www.pgp.org or www.pgpi.org) or GNU Privacy Guard (www.GnuPG.org).

If you favor convenience over a "best-of-breed" approach, as most of us probably will since our focus is on translating and interpreting or fulfilling one of various functions at an agency, it will be easiest to obtain an application suite such as Norton Internet Security (www.symantec.com), which combines an anti-virus program, a personal firewall, and an anti-spam product in one

package. Most of us will probably not need the parental controls application that is also included. At least I would hope that none of you let your children play or work with your personal computer or laptop – doing so could endanger your livelihood, your source of income, and therefore should be off-limits as part of your risk mitigation strategy.

Which brings up another important issue: is your computer safe from your pets? A laptop dripping with coffee your cat knocked over most likely is of very limited use; once it has been cleaned, you might still be able to use it as a paper weight. It's something to think about, just like purchasing an uninterruptible power source (UPS) for your computer(s) to avoid losing valuable work due to a power outage or a brownout. Going into more detail would go beyond the scope of this presentation, if you need advice on these topics, get in touch with the authors.

Several good privacy awareness sites include a privacy analysis web site (www.anonymizer.com/snoop.cgi), ShieldsUp! (grc.com), and Privacy Bird (www.privacybird.com).

If you would like to stay up-to-date on information security topics, you might want to subscribe to some of the SANS Institute's free newsletters (www.sans.org/newsletters):

- SANS NewsBites: General information security news (published weekly)
- SANS PrivacyBits: Privacy-related news (published weekly)
- SANS @RISK: Up-to-date vulnerability information (published weekly)

If you think you do not need to worry about Internet privacy, do a quick search for your name (and its various forms) on Google. We think you will be surprised what you find. Just to play things safe, you might also want to search for your social security number, credit card numbers, and bank account numbers online.