



How-To:

Computer Security For The Rest of Us

<http://www.vermontcomputing.com/>

Intro

This paper is meant to answer some of the many questions on computer security that the average computer user has. It is not a technical paper, and does not cover every detail of computer security. If you have questions on what is written here, please email support@vermontcomputing.com

Spyware

Spyware is a general term that refers to the technology many shareware and freeware software vendors are employing in their products. Generally speaking, spyware collects statistical data about the use of the computer, in relation to the internet, and then sends it back to the company that owns the software. This way, the company can collect the data and sell it to advertisers. These advertisers will often buy a small banner location in the software. That way, you don't pay money for the software, but the company producing it can still make a profit.

The negative side is that information about you is being collected. You may think this is something you never agreed to. However, remember that License Agreement you skipped over without reading? That's a legally binding contract, and you did in fact agree to the terms of it when you installed the software. Your choices are, don't use the software, or accept the consequences.

Not all products that display ads are considered spyware. There are a number of independent organizations on the internet that maintain an archive of products that have spyware built into them. A simple search at your favorite search engine can bring up one of these archives.

You may have heard that a lot of people are up in arms over spyware. For some, it's simply because they are concerned about their privacy, and prefer not to give out any information to anyone. For others, it is the fact that the spyware can collect quite a diverse range of data, and you don't know exactly what it is collecting, and who is getting access to that data.

There are solutions though. You can download, for free, a number of products that remove spyware. One is Lavasoft's (<http://www.lavasoftusa.com/>) AdAware program. It

removes the spyware component of many of today's most popular spyware-utilizing products.

Virii

A virus is a piece of code that uses a computer's resources to spread and replicate. The replication often occurs without the user's knowledge. It can spread via email, or disk (like a floppy disk). All it takes is opening the wrong file, and you can get a virus.

The best way to keep yourself safe from virii is to get a piece of virus protection software, often referred to as antivirus software. Norton Antivirus and McAfee Virusscan are the two most popular products in this category. Either one of them is good protection. Just make sure you keep the program updated. New virii are released daily, and without the most current updates, your computer is not as protected as it could be. Both Norton and McAfee offer a free year of updates with the purchase of their products (they release a new version every year...)

The best way to keep yourself safe from virii is to actually avoid them altogether. If you get an email, with an attachment, and you aren't expecting it, **DO NOT OPEN IT!** I can't fathom the number of times I have offered this advice to people, only to have them ignore it. Weigh the consequences; on the one hand, you could be reading the latest email joke. On the other hand, your computer could wind up needing to be wiped out, and have everything put back, meaning your data is gone. Is that worth the risk? No. I never read email forwards, unless I know why they are there. Knowing the sender is not enough, because many of today's virii will simply send themselves to everyone in your address book. That way, your friends and family see an email from you, trust you, and open it. Then they are infected, too, even though you never intentionally sent them the virus.

Trojan horses/ Remote Administration

Remember the story of the Trojan horse? There are programs that work that way, too. A Trojan horse is any program that does more than it is reported to. Trojan horses are usually employed to install a remote administration tool, such as Sub-7 or the popular Back Orifice. They have legitimate uses, being very powerful tools for controlling another computer remotely. However, the problem comes when someone is controlling the program that you don't want doing so. Remote administration tools can do anything from allow the user to see what is displayed on your screen, to reboot the computer.

Don't fear, though. For most antivirus products can detect remote administration tools attempting to install themselves. So if you follow the previous advice, and keep your system up-to-date, you should be fine.

Anonymity- email, web browsing

Is anonymity possible? To be blunt, no, it is not. However, I should mention that everyone defines anonymity differently. In one sense, it is possible to keep your name, address, telephone number and email address a secret. However, it is not possible to prevent data from being traced back to your computer. This is not meant to be a technical

paper, so I will spare you the details of why certain things can be kept private, and other things cannot.

In order to keep your personal information secret, you want to do a few things:

1. If you are going to email a company for a product inquiry, or are otherwise emailing someone who is not a close friend, you may want to establish a second email address. Companies such as Yahoo! and MSN offer free, web-based email.
2. In that secondary email address, do not put your actual name as the “name” when you set up the email address.
3. Don’t give out your name/address/ etc in IM programs such as AIM or Yahoo! Pager.

Crackers

A “cracker” (also called a “hacker” by the media, yes there is a difference, but it doesn’t matter here) is someone who does malicious things with or to a computer. Crackers can do everything from take control of your computer to make it run slowly. As more and more people use computers, there are bound to be more and more unscrupulous people using them. That means a greater risk for you, the non-malicious computer user.

How much risk is there? Not as much as some would have you believe. With the sheer number of computers out there, it is highly unlikely that you will become a random target. There is a cracker counter-culture that exists today. Part of the reason people attack computers is for status in this world. It is **not** praiseworthy for one of these people to do damage to a random users computer. They would rather go after a company, or a computer reported to be highly-secure. This, combined with sheer numbers is your biggest defense.

If you still want more protection, you can visit www.zonealarm.com and download Zone Alarm. It is a product free for personal use, known as a firewall, that can help to prevent people from accessing your computer. It will notify you if someone tries to do something of the like, and it even has customizable security settings.

Identity Theft

Identity theft is when someone else poses as another person, in some manner, successfully. This is usually with respect to credit cards, or other financial items. Victims of identity theft can spend years proving their case, and retaking their life. On top of that, it can happen to anyone- not just the wealthy. As serious as it is, there are a few things you can do to drastically reduce your risk.

First, use common sense. If someone calls you, and asks for your social security number, or credit card number, don’t give it out. If the product or service being proposed sounds interesting, do a bit of research. Get the company name. Request literature to be sent to you, and ask for a phone number. If the person on the phone says that isn’t possible, then it is most likely a hoax. If their offer sounds too good to be true, it probably is.

Many people are scared about ordering online. However, these same people have no problem giving out credit card numbers in a mail-order form, or over the phone.

Internet ordering is actually the safest of the three! It involves the least amount of human contact, which is where the risk comes in. In these modern times, ALL companies have their customer's information on a computer somewhere. That is not to discourage you from purchasing anything, but instead to make you realize that it is safer than you think. Don't forget, credit card companies stand behind you in cases of fraud- that's their job.

Use a bit of common sense when ordering anything online, and offline. Use a credit card whenever possible (not a checking account, your bank will not back you in the same way a credit card company will).

How to Stay Safe

Simply put, computer security is not the horrible problem the media would have us believe. Yes, there are a lot of problems out there. But that is unavoidable when you consider the number of computers in the world. Know the risks, and be smart. Don't keep a list of your credit card numbers and expiration dates on your computer- there's no need! If you stay cautious, NOT paranoid, you can use your computer and the full capacity of the internet without problem. If you are still concerned, contact a computer consulting firm that understands the risks. Vermont Computing can analyze your security setup and correct the problems for as little as \$25 an hour.