

First National Bank

Internet Security

(An Article from the Internet)

If terms such as 'phishing', 'zombies' and 'DoS' have you thrashing around in the dark, this article will help you get acquainted – and get the upper hand – with these and other online perils.

Table of Contents

1. Introduction	3
2. What Your Up Against.....	3
Viruses and worms	3
Adware, spyware and key loggers	4
Phishing.....	5
Spam	5
Browser hijacking	6
Family, friends and colleagues	6
Zombies and DoS.....	6
3. How You Gain the Upper Hand	7
Pack your toolkit.....	7
4. Shore up your system	9
To combat viruses, worms and similar threats:	9
To keep adware and spyware off your system:	9
To avoid phishing scams:	9
To manage spam:	9
Don't get hijacked:.....	9
To keep others from prying:	9

1. Introduction

Do you ever get the feeling your computing life has degenerated into a constant battle against viruses and spam, spyware and hackers...and you're on the losing side?

You're not alone.

While the past twenty years have seen computers evolve in extraordinary fashion, the safety of the average computer user has been on a downwards spiral for at least the past decade.

Blame it on the popularity and affordability of the humble PC, which has put power into the hands of the many; blame it on the Internet, which connects everyone with everyone else; blame it on the alignment of the planets. No matter who or what you blame, there's no getting around it: computing now is a riskier proposition than it was in the good old days of the '80s and early '90s.

In those ancient times, sighting a real live virus was cause for commotion, and spyware was unheard of. All you needed to do to compute safely was to use anti-virus software and make backups. These days, if your only security tool is an anti-virus program, you're leaving yourself wide open to the vast majority of security risks and privacy threats.

So, should you throw up your hands in defeat and take the PC to the tip? Not on your life. All you need to defeat the forces of evil at their own game is a bit of savvy, a small collection of tools and some commonsense. This article will provide you with the first two and we'll even throw in some guidelines for applying your own good sense.

2. What Your Up Against

Viruses and worms

Viruses used to be the biggest bogey on the Internet. These days, they seem to take a back seat to spyware and spam and phishing scams. But don't let that shift lead you to regarding viruses lightly: get infected with a nasty virus and you'll know the definition of computer hell.

A virus is a small program that infects other code and then replicates. Some viruses also delete or corrupt other files, change computer settings and, in the worst cases, render your computer unusable.

Worms are also self replicating, but they do it alone without attaching to another program as viruses do. The most common form of worm is called a mass-mailing worm. Such a worm uses email to replicate itself. When activated, it may scan your entire computer system for email addresses and then email itself to those addresses. The worm may also place one of the addresses it uncovers into the "From:" field of the infected email, making it seem like it came from a completely different source (a technique known as spoofing the address).

Adware, spyware and key loggers

Adware is software which displays advertising while you use it. Many very useful free utilities and applications use the adware model to raise money. Most adware updates the ads displayed through an Internet connection; some tracks your computer usage in order to target the advertising to your interests.

Spyware is software installed without your knowledge or consent which tracks you while you use the computer and the Internet. Spyware may come piggybacking on other "legitimate" software or it may be installed via a Web site, when you unwisely click a pop-up dialog box to clear it from your screen.



Look for the padlock in your browser's window before entering sensitive data online, and double-click the padlock to ensure the site's security certificate is in order.

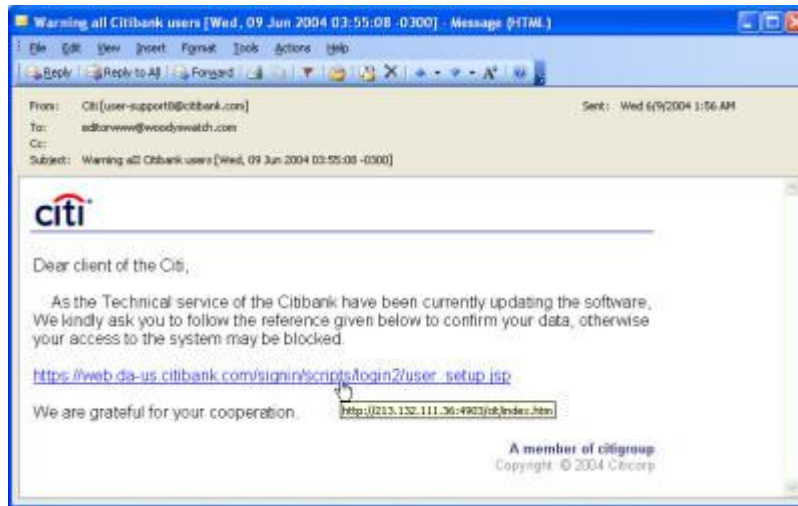
As you might guess, the line between adware and spyware is sometimes measured in nanometres. Things get particularly nasty when spyware not only tracks your usage in order to target advertising, but also to gather personal information about you. In its most pernicious form, spyware may install a key logger on your computer. The key logger lurks hidden on your system and keeps track of every single thing you do, including everything you type. With a key logger active on your system, your security and privacy is completely compromised.

Phishing

Phishers use email and Web sites to try to reel in your private information, including bank account and credit card numbers, PINs and site passwords.

Of course, if you received an email saying "hand over your bank account details", you'd hit the Delete key before you blinked. But what if that email appeared to come from a bank with which you have online access? And what if the email said "There's a problem with your account, if you don't log in and fix the problem we'll suspend account access within 3 days"? And what if, on clicking the link supplied in the email, you found yourself, apparently, at your bank's Web site?

In that case, you might well think the email was on the up and up and complete the log in, in the process handing over your account number and password. Within minutes, the phisher can be working on making you poorer and sullyng your credit record.



Telltale signs of a phishing scam: poor grammar and a fake Web address. (Click the image to see a full-size screenshot.)

That's how phishers work. They fake – spoof – email addresses, email content and Web sites, right down to using the same graphics, wording and other components you find on the legitimate sites. By using some sneaky coding techniques, they can mask Web addresses, fake the padlock security icon on secure pages, and make it difficult, indeed, to spot the fraud.

Spam

We all know spam is a nuisance, but does it rate as a security threat?

Well, apart from the complete invasion of privacy caused by having pornographic spam splattered all over your inbox (and your children's inboxes), the answer is...yes. Many spam emails contain Web bugs – invisible graphics containing tracking code designed for the same purposes as spyware. In addition, the sheer volume of spam and the frustration of having to deal with it may lead to incautious behavior. That is particularly the case when spam is used as the delivery method for a virus or spyware or phishing scam. An unthinking click in the wrong email and, bam!, you've granted entry to the scammers.

Browser hijacking

Browser hijacking is the use of programming tools, in the form of scripts, to modify your browser's default settings. This may be as trivial as adding a new link to your favorites or bookmarks, or as unconscionable as changing your home page persistently via a combination of scripting, registry changes and auto-running programs.

What's the point of hijacking? To bring you back, over and over, to a site or a site's sponsor, in the hope of boosting business. The site to which you are hijacked may also house spyware, and the more often you end up on the site trying to close in-your-face pop-ups and escape, the more chance you'll accidentally install that spyware.

Family, friends and colleagues

If your computer sits in an office shared with others or if your family computes together, there's a risk someone will get interested in what you're up to. Some of those things – tracking financial information, your secret diary, your Christmas purchases – you may not wish to share.

With the threats from viruses and spyware, it's all too easy to forget that some of the biggest threats to your privacy and security are posed by people who can physically get their hands on your computer.

Zombies and DoS

If you've read this far and are thinking "I'm safe – there's nothing on my computer except a bunch of games," have another think. There are people out there who couldn't care less about the information stored on your computer, but they are certainly interested in your computer itself.

Spammers, hackers and virus writers have a vested interest in keeping their identity secret. To stay hidden, one tactic they use is to find unprotected computers on the Internet and use those computers to launch attacks or send spam. Your humble Internet-connected home PC is thus a valuable pawn in their schemes.

Hackers use a piece of code called an agent or daemon to control remote PCs without the owner's knowledge. They then use one or thousands of controlled PCs, known as zombies, to launch attacks on juicier targets. Zombie PCs are crucial in Denial of Service (DoS) attacks, designed to bring the Internet or a part of it to a standstill.

As well as hackers, spammers may find your computer a useful way station. Some spammers seek out vulnerable PCs and, when they find one, install a complete email server on it. They then use this hidden mail server to deliver tens of thousands of spams.

3. How You Gain the Upper Hand

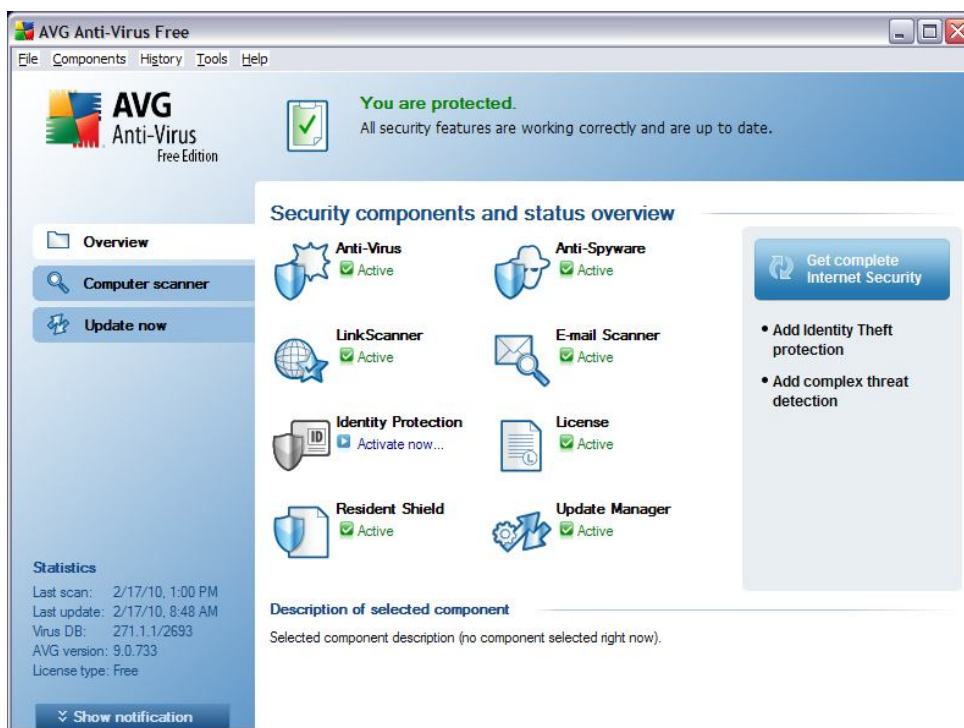
Pack your toolkit

That daunting list of threats may leave you feeling demoralized, certainly weary. The good news is you don't have to fight the onslaught on your own. There are some handy software tools you can use to help secure your system. Keep in mind, though, that even with excellent software defenses installed you'll need to keep your guard up.

While some good security tools are free, be prepared to spend money on securing your computer. This is one area where it doesn't pay to be penny pinching.

So, what should you pack in your security and privacy toolkit? Here's a good starting list:

- Anti-virus software. There are some useful free anti-virus tools, but over the years they have not proved to be the best line of defense. You're better off going with one of the well-known products with a proven track record, such as McAfee Antivirus Suite, PC-Cillin, Norton Internet Security, AVG Anti-Virus Free Edition, or AVG Internet Security. Make sure your anti-virus software protects your email and guards against Web site threats, as well as monitoring your system for infection from other sources. Use your anti-virus program's update feature at least a couple of times each week. (Click the image to see a full-sized screenshot.)



- Anti-spyware and anti-key-logging software. When it comes to anti-spyware tools, adopt the boots-and-braces approach. Because of the rapid proliferation of spyware threats, no software program can keep up with the flow, so it pays to install at least two anti-spyware programs. The good news is, two of the best tools available are free, Spybot Search & Destroy and Ad Aware. Note, though, that the freeware version of Ad Aware is significantly less aggressive than the commercial version. If you're really worried about spyware (and you should be), buy a copy of Ad Aware SE Professional or the equally good Spy Sweeper 3.0.
- A spam blocker. Top choices are Lavasoft's Ad-Aware, Ella and Norton AntiSpam. If you use Microsoft Outlook as your email client, upgrade to version 2003 or 2007 if possible; it has very good built-in junk mail handling. Thunderbird email also has decent junk filters.

- A firewall. A firewall monitors incoming and outgoing traffic between your computer and the Internet, and prevents any unauthorized activity. It's your best defense against being turned into a zombie, and can also trap the activity of spyware and key loggers. Windows XP has a built-in firewall which has been vastly improved with Service Pack 2. Still, it doesn't do a complete job of monitoring traffic, so you should install a third-party scanner instead (don't use two software firewalls concurrently). Check out Zone Labs ZoneAlarm, Outpost Firewall Pro and BlackICE PC Protection. If you have a high-speed, always-on connection, you should consider using a hardware firewall in conjunction with your software firewall. Many cable/DSL routers have a hardware firewall built in. If you are not sure if your router has a firewall call the company that installed it to be sure.
- If you share your computer with others or keep sensitive information on an easily accessible desktop or notebook computer, add password protection to your data. Darn! Passwords is an excellent and affordable password manager which will let you protect your passwords, PINs, serial numbers, account numbers and more.

Your entire toolkit should cost no more than \$200, and probably much less than that as it's likely you already have at least some of these tools installed. If you're starting from scratch, you can reduce the cost by buying one of the security suites, such as McAfee's Internet Security Suite, Norton Internet Security or PC-Cillin. Each of these combines anti-virus, firewall, and anti-spam components with additional features such as anti-spyware or parental controls.

These products can be purchased on-line for download. Be aware that if you are on a dial-up internet service this can be a very lengthy process. You may also purchase these products at most stores that sell computer software and games such as Best Buy, Circuit City, Target, Wal-Mart, EB Games, and computer stores in your area.

4. Shore up your system

In addition to using good anti-virus tools, there are steps you can take to protect yourself and your computer.

To combat viruses, worms and similar threats:

- Beware attachments! Never open an email attachment from someone you don't know. Don't open attachments from people you do know, unless you're expecting the attachment. Don't open attachments directly from within your email: save them to your desktop first and open them from there. Before you open any attachment, right-click it and choose the anti-virus scanning option from the pop-up menu (most anti-virus programs add such an option when you install them).
- Turn the reading/preview pane off. Most email programs display part of an email in a viewing pane beside the list of received email. Switch this viewing pane off. Sometimes your system can get infected merely by displaying code in this window.
- Run a full system anti-virus scan weekly, at a minimum.

To keep adware and spyware off your system:

- Pay for software instead of opting for the free, advertising supported version.
- Avoid surfing on the fringe. Porn sites, crackz and warez (pirated software), file swapping and other on-the-edge sites are havens for unscrupulous people.
- Never, ever click OK on a pop-up window or dialog box when you're browsing without reading it thoroughly. Use the close box to close such windows.
- Use safe emailing practices.

To avoid phishing scams:

- Never click on links in email you receive from an unknown source or from a known source seeking financial or sensitive information. Instead, type the address directly into your browser. Links in email can be dummed to look as if they're taking you one place when they are, in fact, taking you somewhere else.
- If you have any doubt whatsoever about an email apparently from your bank or other financial institution, either go directly to the bank's Web site or get on the phone and speak to someone at the bank directly.
- Be skeptical of any email which asks you to update your log-in details or other sensitive information.
- Never click any link in spam.

To manage spam:

- Never open spam email.
- Never buy anything advertised in spam, even it seems like a really good deal. If you wonder why spammers indulge in a process which seems tailor-made to infuriate potential customers, it's because some people actually buy spam goods.
- Never divulge more information on Web site forms than is absolutely necessary.
- Always read a site's privacy policy before you sign up or purchase goods.

Don't get hijacked:

- Never click OK on pop-up windows online without reading them thoroughly.
- Adjust your browser's settings to prevent ActiveX and JavaScript programs from running.

To keep others from prying:

- Set up multiple logons for your family PC and use a password on each log on.
- Always use strong passwords.