# *Hacked: A Beginner's Guide to PC Security*

**Grace Darling**

My introduction to computer hacking was embarrassing. Some years ago, I inadvertently sent a virus-laden e-mail message to a colleague and fellow CSE member. She very kindly alerted me to the infection and suggested I have my organization's information-technology department provide me with antivirus software. Well, when you are an independent contractor with a home office, you *are* the information-technology department. After learning of the virus I inadvertently spread, I felt like Typhoid Mary, vowed to never let it happen again, and set out to protect my home computer from unwelcome intrusions.

The road to enlightenment is far from smooth. Since that first encounter with a virus, I've been brought to my knees by worms, Trojans, spyware, exploits, and phish. If you own a Windows-based PC and go online, you will be a victim of some form of malware. Like death, taxes, and diverticulosis after age 60, it's inevitable. Viruses and their ilk are not just annoying; they cost businesses and the public millions of dollars a year in lost time and productivity and in computer repairs. Consider the following statistics:

- More than 100 viruses are released daily.
- Symantec claims that Norton AntiVirus protected users from more than 7000 viruses in 2005.
- Computer virus attacks cost global businesses an estimated $55 billion in damages in 2003. That sum was expected to rise every year.
- The median cost to clean up the damage caused by the Blaster worm was $475,000 per company. Some larger, computer-intense companies reported losses of up to $4.3 million.
- Spyware is now considered a bigger threat to business networks than viruses.
- It is estimated that 90% of all PCs harbor 30 or more pieces of spyware.
- Spyware is to blame for half of all PC crashes.
- The UK had the third highest rate of spyware infections in 2005, after the United States and Thailand. The cost to UK taxpayers was in excess of £445 million last year.
- In the United States, the annual cost associated with damage from computer viruses is estimated to be in the billions of dollars.

You can protect your PC by installing appropriate software and keeping it up to date. *FirewallGuide.com*[1] recommends a layered approach, as follows:

1. Choose an Internet service provider (ISP) or e-mail service that offers online virus and spam e-mail filters.
2. Install a wired or wireless hardware router with a built-in firewall between your modem and your computer or network.
3. Install, use, and regularly update personal firewall, antispyware, antivirus, anti-Trojan, antispam, antiphishing, and privacy-protection software on every computer on your network.

The software recommendations given here are based on user reviews and extensive testing reported in major trade publications.

**Table 1. Top-Rated Spam Filters in 2005**

Cloudmark SafetyBar (formerly SpamNet)—Superb detection and low rate of false positives. When any new spam, including phishing-scam e-mails, is reported by users, the spammer is immediately added to SafetyNet's blacklist and universally blocked.

Qurb—Highly effective filter works best for those who receive mail mostly from people they know. If you sometimes receive legitimate mail from people not in your address book, this program is not for you.

MailFrontier Desktop—As effective as SafetyBar but requires users to configure the software to their preferences. Reviews say its antiphishing tools don't work as well as SafetyBar's.

SpamSieve—One of the few spam filters available for Mac users.

iHateSpam—Very popular with users but ranks low in *PC Magazine*'s tests because of a 20% false-positive rate. *PC World*'s reviewers note some system lag.

## Spam Filters

Spam, or junk e-mail, is unwanted commercial solicitation. The first spam e-mail was sent in 1978, and now spam accounts for billions of messages every day. For one-third of all e-mail users, about 80% of the messages received are spam. According to Goodman and colleagues,[2] spam has proliferated so freely because it is extremely cheap to distribute: They estimate that a message costs about 0.01 cent to send. "At these cut-rate prices a spammer can earn only $11 per sale and still make a profit, even if the response rate is as low as 1 in 100,000. Hence, although very few e-mail users ever buy anything advertised in spam, all of us suffer because of those who do."[2]

Most ISPs offer spam filters as part of their signup package. For instance, my ISP offers Web-based Yahoo!Mail to its subscribers. The Yahoo!Mail spam filter combined with the filters provided by

GRACE DARLING *is a manuscript editor by day and an inveterate tinkerer in the dark of night.*

*Hacked continued*

the Eudora e-mail client and Norton Internet Security Suite does an excellent job of blocking unwanted messages. About once a week, I review the contents of my Yahoo!Mail Bulk mailbox and delete the junk mail. Only rarely do I find a legitimate message mislabeled as spam—maybe 1 in over 300 e-mails. Nevertheless, industry reviewers claim that these packaged filters are not as robust as standalone products (Table 1).

**Table 2. Top-Selling Antivirus Programs in 2005**

Shield Pro 2005/2006—Available only over the Internet for immediate download; comes with a built-in firewall, 12 bonus issues of *PC Magazine*, and free unlimited support. This inexpensive program is easy to install and use; reviewers call it the "perfect program for the less computer savvy".

BitDefender 9—A good value with fast and effective scans, simple interface, and preset updates; a good "install and forget" program. Comes with a lot of bells and whistles, some of which can be annoying but can be turned off. No customer support by telephone, only via chatroom and e-mail.

McAfee VirusScan and Norton AntiVirus—The two biggest players in the antivirus business. They install quickly and easily and are meant to integrate with their own parent company's Internet security suites. McAfee uses rather a lot of memory to operate but stopped the test viruses cold. It has no telephone technical support. Norton was also very good at virus detection and removal but is the most expensive. Phone support costs $29.95 per incident; online and e-mail support is free. Both must be renewed yearly.

Kaspersky Online Scanner, VirusTotal, Jotti Online Malware Scan—Virus detection only, no cleaning or deletion, but fast and efficient for checking e-mail attachments for viruses and Trojans without having a resident program that takes up your system resources. Their scan engines use different techniques, and experts advise that you use more than one.

## Antivirus Programs

Viruses are transported via e-mail, so before you open your new messages you should check who sent the e-mail and whether it has attached files: Attached files carry viruses. If you don't recognize the e-mail sender's name, delete the message without opening it. If you recognize a friend's or colleague's e-mail address but don't know what the attachment contains, check before opening the file: The virus itself could have sent you the message from your friend's e-mail address. A virus may be lurking in a joke, image, or other document, and opening the attachment could infect your computer and spread the virus to all the addresses in your address book.

Antivirus software can be extremely effective in scanning the e-mails received and sent (Table 2) but must be kept up to date. Daily, or at least weekly, downloads of the latest virus definitions will keep your PC reasonably protected from infection. Most software manufacturers recommend the automatic live-update function that runs in the background. At the University of Texas Southwestern Medical Center, virus definitions are updated hourly for all computers in the network. At home, you can adjust the update settings to fit your level of paranoia.

Despite those protective measures, Microsoft[3] warns that "no anti-virus software is completely failsafe". The best way to avoid any lasting damage to your computer is to regularly back up your files. If a virus hits your computer, most of the software can be reinstalled, but your personal files will probably be lost. Once the virus is removed and your PC is clean again, you can restore it to its preinfection status from the backup files.

## Firewalls

A software firewall enforces an access-control policy between two or more computers and basically acts as a virtual gate for your PC, at times blocking traffic and at other times permitting entry to your system. Firewalls provide a single "choke point" where security audits take place and are generally configured to protect against unauthenticated interactive logins from the Internet—malware attacks. When you first set up a software firewall, you can specify which applications are allowed to communicate over the Internet from that PC. Either programs that are not explicitly allowed to do so are blocked or the user is prompted before the traffic is allowed to pass.

An October 2004 industry survey[4] found that 72% of computer users had an open port through which a hacker could gain access to their files. Even among broadband users, 50% lacked a firewall, yet 84% kept sensitive health or financial records on their computers and 72% did their banking online.[4] A firewall has to know which interactions between the PC and the Internet are safe (Table 3). Most firewall programs cannot do this on their own and must be configured by the user. Creating an approved list of interactions can be confusing.

Security suites, such as those offered by Norton and McAfee, typically combine spam filters, antivirus software, a personal firewall, antispyware, and parental-control filters in one program. You may already have some of those features installed in your PC, in which case a standalone firewall may be all you need.

A software firewall can protect only the computer it is installed in, so if you have multiple computers you need to install and configure a firewall separately for each machine. Computer experts warn not to

**Table 3. Firewalls**

Security Suites

ZoneAlarm Security Suite—Reviewers recommend this program above all others. It offers protection from identity theft by warning about phishing e-mails plus and pop-up blocking and antivirus capabilities. Editors praise its superb firewall, spam filter, and ease of use: ZoneAlarm automatically preapproves popular programs when checking the Internet for updates and other safe interactions. The privacy settings can be readily adjusted to suit your online habits. Critics fault its spyware detection and recommend installing a separate antispyware program.

PC-cillin Internet Security 2005—Another frontrunner in the security suite field among professional reviewers. It includes first-rate antivirus, firewall, antispam, and spyware-blocking tools plus a host of other security features at a lower price than its competitors. Users praise how PC-cillin works in the background without slowing their computers. The 2005 version includes warnings of phishing e-mails and of intruder attacks. For wireless users, the software includes protection for all the PCs on a home network. Some reviewers criticize its easily bypassed parental controls and note that its firewall and antispyware tools fail to do the job properly.

Norton Security Suite and McAfee Internet Security 2005—Although these two programs command the lion's share of the market, their firewalls failed various industry tests, and both are downgraded because of their heavy use of system resources. Users complain of installation nightmares, incompatibilities with other programs, and severe system slowdowns—annoying enough to cause some users to disable the security suites entirely.

Standalone Firewalls

Windows XP Service Pack 2—Installs a security center that allows you to control Windows Firewall as well as third-party firewalls and antivirus applications you may have running. It has a pop-up blocker for Internet Explorer, and the firewall blocks incoming attacks very well, but it doesn't block outbound traffic from your computer, which can be a problem if you are inadvertently harboring an unauthorized application.

Outpost Firewall Pro—Very popular in Europe but practically unknown in the United States. Editors praise its combination of a powerful feature set and easy-to-use design. One of the few firewalls that passed every test. Reviewers give it the highest possible rating, and users mostly agree.

Sygate Personal Firewall, Kerio Personal Firewall, BlackICE Defender—These standalone products are most often mentioned in user surveys. Each has its fans and detractors, but they all share dynamic protection filters that "analyze network traffic and detect and block suspicious patterns". Sygate is free, easy to use with default settings, and said to be extremely effective. Kerio Personal Firewall was discontinued in 2005 and will be succeeded by Kerio WinRoute Firewall. Faithful users like its small footprint and faultless performance. BlackICE offers four security levels: Trusting, Cautious, Nervous, and Paranoid. That bit of whimsy alone is reason to like it.

try to run more than one firewall in your PC at the same time; this can cause conflicts and system crashes.

## Routers

Some security consultants recommend using a router as the first line of defense even if your PC is not on a network, to capitalize on the router's built-in firewall.[5] If your home office computer has a high-speed (DSL or cable) Internet connection, "a hardware firewall [router] should be considered a bare minimum, and supplementing it with a software firewall on one or more computers (and don't forget anti-virus software) is almost always a good idea".[6]

A router organizes and directs data traveling between computers or networks. Routers are installed between the modem and the computer and serve as an Internet connection sharing point, allowing multiple computers on the home network to access the Internet simultaneously. An NAT router obtains a single IP address from the manufacturer and hides the real IP addresses of all the computers connected to it, rendering them invisible to potential attackers and much less likely to be hacked. The routers used to connect a small office network to the Internet enforce rules concerning security for all the computers in the network regardless of platform—that is, they work equally well whether the PCs run Windows, Mac, Linux, Unix, or any combination of these.

Not only do routers act very much like a firewall, but some routers also have firewall software built in. The most popular brand names in the United States are Linksys, Netgear, D-Link, and Buffalo. Prices range from $15 for a basic model to $100+ for a wireless router with a full set of features that appeal only to the technically inclined. Generally, routers are effective, easy to install and set up, and inexpensive.

Wireless routers are actually wired routers with wireless access points built in so you can have wired and wireless connections in the same network at the same time. Because wireless routers are not as secure as hard-wired ones, in 2006 all buy-

*Hacked continued*

ers of Linksys routers will receive Norton Internet Security Suite 2006 bundled with their purchase to further protect them from online attacks.

### Spyware Removal Programs

Spyware is software that gathers personal information from your computer without your knowledge. It may cause your computer to slow down or crash, be unable to connect to the Internet, or have problems with printing. In its benign form, spyware manifests as pop-up advertisements, unwanted links, and redirected searches—adware. A more sinister type of spyware includes system monitoring tools that record every site you visit online and keylogger programs that capture keystrokes to gather information about e-mail addresses, passwords, bank accounts, and credit-card and Social Security numbers.

A common way to fall victim to spyware is to install file-swapping programs for downloading music and movies from the Internet. "Misspell a common URL and you are likely to land on a domain that will inject spyware into your PC", says an industry expert. "For users today, it is difficult to avoid getting spyware if you surf the Net at all."[7]

Because most spyware is not delivered via e-mail, antivirus products are ineffective at detection. In addition, no single detection tool seems to be able to detect all spyware; new and mutating spyware programs are being written every day, and security experts are in a constant race to keep up with spyware writers.

Spyware removers can tell you what has infected your PC but cannot prevent infection in the first place, and spyware can be nearly impossible to remove with even the most sophisticated tools (Table 4). Some spy programs are designed to reinstall themselves once removed, maintain multiple copies simultaneously, make thousands of entries to the Windows registry, and thwart detection by antispyware products.

There is even a notorious bandit that masquerades as a spyware remover. Spy Sheriff is a system hijacker that causes pop-ups to appear on your monitor telling you that you have spyware installed in your PC. Clicking on the alert brings you to a Web site that attempts to sell you a bogus antispyware program called—you guessed it—Spy Sheriff. A similar scam is perpetrated by *securitycaution.com*, which will claim that your PC is infected by a worm and point you in the direction of a couple of fake spyware removal tools.

Because even the highest rated Spyware Doctor achieves a detection rate of only 84% and a removal rate of 73%, security experts recommend that you run at least two antispyware programs in tandem to bridge the gap in coverage.

**Table 4. Spyware Removal Programs**

Webroot's Spy Sweeper, PC Tools Spyware Doctor 3.2, Aluria Anti-Spyware, CounterSpy, Trend Micro Anti-Spyware—There is little difference between these products, all of which do a fair job of identifying and removing spyware from your system—average 73% removal rate—at prices ranging from $20 to $30. Each has its own quirks. For example, Spy Sweeper is a resource hog that bombards you with constant pop-up alerts, and Spyware Doctor has no automatic updates, the scheduler has to be set up manually, and removal takes much longer than for other programs.

SpyCleaner 8.7, WinPatrol 9.8.1, HijackThis 1.99.1*—These are all popular because they are easy to use, moderately efficient, and fast. They typically scan the Windows registry and hard drive, detect spyware, back up infected files (in case they are false positives that must be restored later), and remove them.

Spybot*—The only freeware in its class, Spybot has serious limitations in features, and updates are infrequent, but it does the basic job of detecting and removing spyware with a minimum of fuss.

*Despite reviewers' preferences, PC users give top marks to these.

### Adware Removal Programs

Pop-up advertisements and unintended links cost PC users considerable time and money and slow a PC's overall performance substantially. Unlike spyware, which burrows stealthily into your hard drive, adware tries to sell you something with pop-up ads and hijacked browsers to commercial sites. Some users accept adware as a small price to pay in exchange for the benefits of weather updates, traffic reports, or stock quotes. For information on adware removal programs, see Table 5.

### Antiphishing Tools

Phishers create a replica of an existing Web page to fool users into submitting personal, financial, or password data. Phishing attacks can use spam, viruses, Trojans, worms, spyware, keyloggers, and other malware. To protect yourself, you must use a personal firewall and antivirus, anti-Trojan, antispyware, antispam, antiphishing, and privacy software (Table 6) plus healthy measures of skepticism and common sense.

Probably the most effective and least costly defense against theft of personal data is your behavioral modification. You should routinely

- Check that a Web site is secure before you enter personal information or credit details. A padlock icon in the bottom corner of your browser lets you know that the site uses secure encryption of the data to prevent theft.
- Never include passwords or credit details in an e-mail.
- When informed of some problem with a transaction that requires you to resubmit personal data, go directly to the company's customer service Web page; do not follow the links provided by the prompting e-mail.
- Create strong passwords and keep them safe (Table 7).

### Pharming

"Phishing is to pharming what a guy with a rod and a reel is to a Russian trawler", said Chris Risley, an industry expert. Whereas phishing requires active participation by the victims, who must respond to phony e-mails and provide confidential information about themselves, pharming works invisibly, and most people are unaware that they are being scammed. And the profit potential for pharmers is enormous.

Infiltrating a user's PC primarily through shareware, freeware, and some commercial programs, pharmers plant Trojans that "poison" the domain name system (DNS), which translates URL and e-mail addresses into numeric strings. A computer with a poisoned server will be directed to the villain's Web site even if a user types in the correct URL. The bogus site to which victims are sent without their knowledge looks the same as the genuine site, and as far as the browser is concerned, it is connected to the right site. But when users log in—with name and password, and often Social Security, credit-card, and bank-account numbers—impostors capture the data. The danger of pharming is that you no longer have to click an e-mail link to hand over your personal information to identity thieves; in fact, you won't even know you've been robbed.

This sort of domain spoofing has been around for a long time, but in 2005 a spate of attacks made pharming front-page news. According to the SANS Institute's Internet Storm Center, pharmers exploited a vulnerability in Norton's firewalls to redirect users trying to reach Google, eBay, and weather.com to three malicious sites. Symantec issued a fix, and other Internet security companies are following suit.

Meanwhile, a partial solution is to access Web sites only via secure connections. A small padlock icon in the lower right corner of the screen indicates that the merchant has obtained an SSL certificate for maintaining a secure connection with data encryption at both ends. This approach depends on users noticing the lock icon and refusing to deal with sites that don't use secure connections; eventually sites that don't display SSL certificates would be driven out of business.

**Table 5. Adware Removal Programs**

XoftSpy Scan—Detects the widest variety of spyware, adware, and other threats on industry tests. Very easy to use and thorough; offers free updates. The top choice of several reviewers.

NoAdware—Easiest to use, with a very user-friendly interface. Gets the job done efficiently and quickly. Scans PCs for spyware, adware, dialers, and Web bugs. Automatically blocks pop-up ads and Yes-No windows that ask for access to your system to download malware. Can be configured for regularly scheduled or one-time scans.

Poper Killer—Stops all pop-ups and ads before they load, and lets you view the number of pop-ups blocked. Blocks plug-ins and ActiveX installers. Easy to install, customize, and use, with 24/7 live technical support—and it's inexpensive.

Lavasoft Ad-Aware SE—A long-time freeware favorite. The standard edition is a huge improvement over previous versions but still lags behind other programs in effectiveness. Its Pro and Plus editions are pricey and not worth it.

### Keylogging

Keystroke capture, or keylogging, is a form of phishing that can be accomplished by hardware or software. Many devices and programs are available commercially and are popular among businesses to prevent unauthorized use of their computers by staff and in law-enforcement circles. (The Federal Bureau of Investigation used a keylogger program called Magic Lantern to track a suspected criminal in Philadelphia.) Apparently, writing software applications for keylogging is a simple matter, and the malicious code can be distributed as a Trojan or as part of a virus or worm hidden inside ordinary software downloads, e-mail attachments, or files shared over networks.

In some countries, keylogging is considered a bigger threat to Internet security than viruses and phishing scams. In the United States, the SANS Institute estimates that in late 2005 as many as 10 million PCs "were infected with keyloggers of one kind or another, putting as much as $24 billion in bank-account assets—and probably much more—at the fingertips of fraudsters". Some researchers believe that the infection rate is probably much higher.

Your means of defense are the usual: make sure to install antispyware, antivirus, and personal firewall programs; keep them current on signatures and definitions; and scan your system often. Don't forget to download Windows updates, especially Security Pack 2. Most major commercial products will seek out keylogging Trojans, and some tools, such as Spyware Doctor

**Table 6. Often-Mentioned Tools to Combat Phishing**

*Free tools*
CallingID Toolbar
Earthlink Toolbar featuring ScamBlocker
FraudEliminator
SpoofStick versions for Internet Explorer and Firefox
Webroot's Phish Net beta

*$20 to $40 yearly*
Clear Search Anti-Phishing
Cloudmark SafetyBar for Outlook and Outlook Express
MailFrontier Desktop

## *Hacked continued*

and SpySweeper, are said to be particularly adept at detecting such intrusions. A couple of dedicated products, Anti-Keylogger and PrivacyKeyboard, have entered the market recently, and their effectiveness is not clear as of this writing.

Free copies of Norton Antivirus 2005, Ad-Aware SE Personal, and Spybot are available for download as part of Google Pack. Microsoft Defender, the giant's anti-spyware response to Internet security gaps, is also free as of this writing.

*Windows updates are necessary to help prevent problems with viruses, worms, etc. However, they should be used in combination with constantly updated virus definitions, firewalls, parasite removal, and frequent backups of your important data. It takes a combination of all of these to keep you, and your computer, happy and functional.*

Tech Talk[8] (October 2003)

**Table 7. Managing Your Passwords**

- Use different user names and passwords to access your various Internet accounts.
- Avoid using variations of your name and your birthday. Never use your Social Security number or bank PIN.
- User name should always be a nickname, not a real name.
- A strong password is at least eight characters long and contains a random mixture of numbers, upper- and lowercase letters, and symbols.
- Keep a written record of your various passwords in a safe place—for example, in a small address book or on Rolodex cards. Some experts recommend password-managing software, such as Account Logon or Acerose Password Vault, which provide you with a single user name and password for all your online accounts and encrypt all information related to this Web site. Do not create a password file on your computer, because it can be hacked.

### Acknowledgments

Special thanks to Judy Dickson for her firm editing hand and expert reorganization of a mediocre first draft. Thanks also to John Darling and Seth Beckerman for reviewing the manuscript and offering helpful suggestions.

### References

1. Home PC Firewall Guide. *www.firewallguide.com/*. Accessed 18 January 2006.

2. Goodman J, Heckerman D, Rounthwaite R. Stopping spam: what can be done to stanch the flood of junk e-mail messages? ScientificAmerican.com April 2005 issue. scientificamerican.com/article.cfm?chanID=sa006&colID=1&articleID=000F3A4B-BF70-1238-BF7083414B7FFE9F. Accessed 18 January 2006.

3. Security at Home. www.microsoft.com/athome/security/default.mspx. Accessed 18 January 2006.

4. Firewalls—Internet Security Software. www.consumersearch.com/www/software/firewalls/fullstory.html. Accessed 18 January 2006.

5. Gottesman B. Keep your PC safe: learn to wield your firewall, antivirus, and antispyware tools expertly; don't give up your PC without a fight. www.pcmag.com/article2/0,1759,1618797,00.asp. Posted 3 August 2004; accessed 18 January 2006.

6. Pacchiano R. Can you ever be truly safe and secure online? Troubleshooting Q&A. www.practicallynetworked.com/qa/qa20041117.shtml. Posted 17 November 2004; accessed 18 January 2006.

7. Tim Powers, cited in Spyware: IT's public enemy No. 1. techrepublic.com.com/5100-22-5543466.html?tag=nl.e101. Posted 20 January 2005; accessed 18 January 2006.

8. Tech Talk, October 2003, Sarasota PC Users Group. www.spcug.org/reviews/bl0310.html. Accessed 18 January 2006.