

Mac Security 101

Even though much of the publicity surrounding viruses, Trojan horses, and other Internet security threats focuses on the Windows platform, Macs can be just as vulnerable to these attacks as PCs are. This unbalanced attention often results in unprotected Macs that are left open to hacker warfare, stolen information, and virus infection because the owner was unaware he or she was vulnerable. To make matters worse, hackers are aware of this chain of events and are beginning to exploit it to their advantage. As a Mac owner, you must be aware of the common dangers you may encounter while computing, and learn how to protect yourself against them.

Hazardous Residents

- **Viruses.** You've downloaded and installed a screensaver from the Internet and, suddenly, your computer is behaving strangely. You're sure you saved that financial document -- but it's nowhere to be found. And other files begin disappearing. If you're lucky, the virus you've contracted might award you with a message bragging of its presence - a text box, song, or video clip. Or it might hide in the depths of your Mac, wreaking havoc slowly and invisibly. Soon it will begin doing what viruses do best: making copies of itself to spread to other machines. Luckily, viruses cannot simply attack your machine - the virus needs the file it is attached to in order to survive, and it needs you to open the file in order to be executed. This is good news: If you follow safety guidelines and run anti-virus software on your Mac, you won't have to worry about where your files are disappearing to or why the diskette that was full yesterday is blank today. And even though viruses are not as widespread in the Mac OS as in Windows, your "virus-free" Mac may unknowingly pass PC viruses to friends and coworkers, wreaking havoc on their systems and important files.
- **Trojan horses.** The Trojan horse's most insidious characteristic is its ability to masquerade as a harmless program, like a cartoon or birthday card, which recipients would not think twice about running. Once downloaded and executed, these programs can create "back doors" in your system that allow hackers access. One example is a Trojan horse called BackOrifice that, once opened, provides a hacker with complete and total access to your computer. BackOrifice allows the hacker to see keystrokes, steal passwords, and run programs. Since this program is almost undetectable, it is hard to know if you have it running on your system or not. And even if you could see it, it's difficult to remove.
- **Worms.** "Melissa" and "ILOVEYOU" are highly publicized, destructive worms that spread, as many worms do, through the use of email. Worms are deceiving and often come disguised as a benign attachment or game. To disguise itself, the Melissa worm used the victim's address book to masquerade as an email from a friend or coworker. Recipients recognized and trusted the sender and, therefore, opened the email attachment. Worms can also get into your system through file sharing, like on the online MP3 trading community, Napster. Instant messaging programs like ICQ can also be an entryway for worms, as well as programs downloaded from the Internet. Just like a virus, a downloaded or contracted worm must be executed in order to cause damage. Its antics may include renaming and hiding your documents, erasing data, or replacing files with replicated versions of itself.

The Eviction Notice

A quality anti-virus software package, such as Symantec's Norton AntiVirus, is your first line of defense to protect your Mac from viruses and their cousins, the worm and the Trojan horse. Anti-virus software scans files regularly for unusual changes in file size, programs that match the software's database of known viruses, suspicious email attachments, and other warning signs. It's important to use your anti-virus program all the time for it to be effective -- you can have it start when you boot up and continue running in the background while you surf the Web and work on your computer. Anti-virus software only works if you keep it up to date - and new virus definitions come out almost daily. Norton AntiVirus makes keeping your protection current easy with its LiveUpdate feature, which automatically brings you new virus updates so you are always protected.

In addition to protecting your Mac with Norton AntiVirus, you should follow these guidelines to further protect your computer from a virus, worm, or Trojan horse invasion:

- Don't open email from an unknown source.
- Only open expected attachments and scan them with Norton AntiVirus before opening it.
- Be sure your email program doesn't automatically download attachments. This will ensure that you can examine and scan attachments before they run.
- Unless you know and trust the source, do not download programs or software from the Internet. If you must do so, download the file into a separate folder on your hard drive and scan it with anti-virus software before running it.
- Update virus definitions frequently. Keep your virus definitions current by updating your anti-virus software at least every two weeks.

In the event that you do contract an uninvited visitor, the Symantec AntiVirus Research Center (SARC) can help you get rid of it. SARC regularly posts programs you can download to remove viruses, worms, and Trojan horses from your computer. The programs scan your hard drive for unusual changes and reverses them, cleaning up the worm in the process.

Hackers & Firewalls

Hackers don't just target high profile companies and banks for their trespasses. As a matter of fact, many of the hackers who successfully bring down big corporations first learned to hack by breaking into personal computers. Tomorrow's Yahoo assailants could be cutting their teeth on your household Mac -- unless you're prepared to stop them.

Hackers have a battery of tools they use to gain access to your computer. They program other computers to scan the Internet at the speed of light for unprotected machines, and they write utilities to do their dirty work. So if you want to keep your Mac safe from prying eyes, you need something to hide behind. In most cases a firewall will do the trick.

Firewall software serves as a kind of door guard for all the information coming into and going out of your computer. A firewall examines the data entering your computer from your Internet connection and compares it to criteria that you have specified during configuration, screening out suspicious activity such as oversized files. Norton Personal Firewall is an easy way to protect your computer's Internet connection, protecting your Mac against many different kinds of intruders and keeping your personal data safe. If you have an always-on connection to the Internet such as DSL or cable, a firewall is imperative for protection against hackers because your computer's constant connection makes it easier to target.

Passwords

You probably have more than one password to worry about, especially if you spend a lot of time on the Web. One word for your email program, one for your Internet service provider, newsgroups, "members only" areas of popular sites, bank accounts, online shopping carts . . . the possibilities are endless. Many people make their lives easier by picking one simple password - their dog's name, for example -- and using it for all of their logins. Unfortunately, this shortcut also makes hackers' lives easier when they're trying to break into your accounts.

For best password security:

- Use both numbers and letters, a mix of upper- and lowercase letters, and punctuation if possible.
- Avoid using names or recognizable dates such as your birthday.
- Don't write it down - memorize it. This is especially important at work where others can take scraps of paper from your desk while you're away from it.
- Change your passwords often. The more frequently you change them, the more difficult they are to crack.

If you have a hard time remembering all of your alphanumeric concoctions, there are programs and online services that allow you to securely store all of your passwords and access them with one single key - the only password you really have to remember. Although it may seem inconvenient to go to all this trouble for passwords, when it comes to your online security, you should take whatever steps you can to protect your personal information. Just think of the damage your online banking password could do in the wrong hands.

Now that you know what security breaches your Mac is vulnerable to, you can begin protecting it. Norton Personal Firewall and Norton AntiVirus are available together as part of Norton Internet Security, your complete online security suite for the Macintosh. Protect your computer, your personal information, and your sensitive data from prying eyes and malicious code and your online experience will be safer and more enjoyable for you and your Mac.

[Tell a friend about this article.](#)

[Return to the Symantec Macintosh Security Site](#)