# Keeping online criminals at bay

*As hacking becomes more lucrative and harder to detect, it is now more important than ever to protect yourself from malware and other attacks on your computer*

BY **RIVA RICHMOND**
NY TIMES NEWS SERVICE, NEW YORK

The Web is a fount of information, a busy marketplace, a thriving social scene — and a den of criminal activity.

Criminals have found abundant opportunities to undertake stealthy attacks on ordinary Web users that can be hard to stop, experts say. Hackers are lacing Web sites — often legitimate ones — with so-called malware, which can silently infiltrate visiting PCs to steal sensitive personal information and then turn the computers into "zombies" that can be used to spew spam and more malware onto the Internet.

At one time, virus attacks were obvious to users, said Alan Paller, director of research at the SANS Institute, a training organization for computer security professionals. He explained that now, the attacks were more silent. "Now it's much, much easier infecting trusted Web sites," he said, "and getting your zombies that way."

And there are myriad lures aimed at conning people into installing nefarious programs, buying fake antivirus software or turning over personal information that can be used in identity fraud.

"The Web opened up a lot more opportunities for attacking" computer users and making money, said Maxim Weinstein, executive director of StopBadwarea nonprofit consumer advocacy group, which receives funding from Google, PayPal and Mozilla, among others.

Google says its automated scans of the Internet recently turned up malware on roughly 300,000 Web sites, double the number it recorded two years ago. Each site can contain many infected pages. Meanwhile, malware doubled last year, to 240 million unique attacks, according to Symantec, a maker of security software. And that does not count the scourge of fake antivirus software and other scams.

So it is more important than ever to protect yourself and others from attackers. Here are some basic tips for thwarting them.

### PROTECT THE BROWSER

The most direct line of attack is the browser, said Vincent Weafer, vice president of Symantec Security Response. Online criminals can use programming flaws in browsers to get malware onto PCs in "drive-by" downloads without users ever noticing.

Internet Explorer and Firefox are the most targeted browsers because they are the most popular. If you use current versions, and download security updates as they become available, you can surf safely. But there can still be exposure between when a vulnerability is discovered and an update becomes available, so you will need up-to-date security software as well to try to block any attacks that may emerge, especially if you have a Windows PC.

It can help to use a more obscure browser like Chrome from Google, which also happens to be the newest browser on the market and, as such, includes some security advances that make attacks more difficult.

### GET ADOBE UPDATES

Most consumers are familiar with Adobe Reader, for PDF files, and Adobe's Flash Player. In the last year, a virtual epidemic of attacks has exploited their flaws; almost half of all attacks now come hidden in PDF files, Weafer said. "No matter what browser you're using," he said, "you're using the PDF Reader, you're using the Adobe Flash Player."

Part of the problem is that many computers run old, vulnerable versions. But as of April, it has become easier to get automatic updates from Adobe, if you follow certain steps.

To update Reader, open the application and then select "Help" and "Check for Updates" from the menu bar. Since April, Windows users have been able to choose to get future updates automatically without additional prompts by clicking "Edit" and "Preferences," then choosing "Updater" from the list and selecting "Automatically install updates." Mac users can also arrange updates using a similar procedure, though Apple requires that they enter their password each time an update is installed.

Adobe said it did not make silent automatic updates available previously because many users, especially at companies, were averse to them.

To get the latest version of Flash Player, visit Abobe's Web site.

Any software can be vulnerable. Windows PC users can identify vulnerable or out-of-date software using Secunia PSI, a free tool that scans machines and alerts users to anything that needs attention.

### BEWARE MALICIOUS ADS

An increasingly popular way to get attacks onto Web sites people trust is to slip them into advertisements, usually by duping small-time ad networks. Malvertising, as this practice is known, can exploit software vulnerabilities or dispatch deceptive pop-up messages.

A particularly popular swindle involves an alert that a virus was found on the computer, followed by urgent messages to buy software to remove it. Of course, there is no virus and the security software, known as scareware, is fake. It is a ploy to get credit card numbers and US$40 or US$50. Scareware accounts for half of all malware delivered in ads, up fivefold from a year ago, Google said.

Closing the pop-up or killing the browser will usually end the episode. But if you encounter this scam, check your PC with trusted security software or Microsoft's free Malicious Software Removal Tool. If you have picked up something nasty, you are in good company; Microsoft cleaned scareware from 7.8 million computers in the second half of 2009, up 47 percent from the 5.3 million in the first half, the company said.

Another tool that can defend against malvertising, among other Web threats, is K9 Web Protectionfree from Blue Coat Systems. Though it is marketed as parental-control software, K9 can be configured to look only for security threats like malware, spyware and phishing attacks — and to bark each time it stops one.

### POISONED SEARCH RESULTS

Online criminals are also trying to manipulate search engines into placing malicious sites toward the top of results pages for popular keywords. According to a recent Google study, 60 percent of malicious sites that embed hot keywords try to distribute scareware to the computers of visitors.

Google and competing search engines like Microsoft's Bing are working to detect malicious sites and remove them from their indexes. Free tools like McAfee's SiteAdvisor and the Firefox add-on Web of Trust can also help — warning about potentially dangerous links.

### ANTI-SOCIAL MEDIA

Attackers also use e-mail, instant messaging, blog comments and social networks like Facebook and Twitter to induce people to visit their sites.

It's best to accept "friend" requests only from people you know, and to guard your passwords. Phishers are trying to filch log-in information so they can infiltrate accounts, impersonate you to try to scam others out of money and gather personal information about you and your friends.

Also beware the Koobface worm, variants of which have been taking aim at users of Facebook and other social sites for more than a year. It typically promises a video of some kind and asks you to download a fake multimedia-player codec to view the video. If you do so, your PC is infected with malware that turns it into a zombie (making it part of a botnet, or group of computers, that can spew spam and malware across the Internet), exposes your personal information and possibly imperils your friends.

Spam filters and current security software can help protect you. Defensioa tool from Websense that is free, can block spam and malicious links from being posted on your blog or Facebook page.

On May 13, Facebook unveiled new security features to combat malware attacks, phishing scams and spam.

Users can choose to be notified when their account is accessed from a computer or mobile device they haven't used before. To do this, go to "account settings," then "account security," then click change. There you can choose to be notified of logins by e-mail or text message.

Facebook is also adding a layer of authorization when it notices unusual activity on an account, such as simultaneous log-ins from opposite sides of the planet. The changes, which are currently being rolled out, come as Facebook faces increasing criticism over the way it handles user privacy.

Above all else, you need to keep your wits about you. Criminals are using increasingly sophisticated ploys, and your best defense on the Web may be a healthy level of suspicion.

ADDITIONAL REPORTING BY AP

The Google and Facebook Web sites are displayed on laptop computer monitors last month. Google says its automated scans of the Internet recently turned up malware on roughly 300,000 Web sites, double the number it recorded two years ago. Facebook, which faces increasing criticism over the way it handles user privacy, earlier this month rolled out new security features to combat malware attacks, phishing scams and spam. PHOTO: BLOOMBERG

## Internet privacy: Should we be sharing our life on the Web?

BY **GARETH MURFIN**
CONTRIBUTING REPORTER

Our attitudes toward sharing information on the Web have changed dramatically over the past 10 years. MySpace, Facebook and Twitter now allow us to keep our social networks updated with the most mundane of information. Why are these sites so popular and why are we so willing to share what we had for breakfast with the world? More importantly, what are the ramifications of sharing this type of information?

In the early 1990s, people were afraid to shop online. It was assumed that entering credit card details over the Internet was risky, but in fact it was and always has been more secure than giving your details out over the phone. Data taken over the Web is encrypted, and even the owners of the site can't tell you your password or credit card number if they wanted to.

As the Internet has developed, people have become less wary. Gone are the days when identify theft was considered a major concern, when users expect to be ripped off on eBay or to have their credit card details stolen and distributed when shopping online. When Amazon.com, for example, started to recommend purchases to its users based on their shopping and browsing habits, this was considered by many to be a breach of privacy. Now it's something we expect on all good shopping sites. When Google told the world it would provide relevant advertisements inside Gmail — for instance, if you are talking about carnations, it might suggest a local florist where they can be bought — the knee-jerk reaction was to assume that Google was monitoring users' e-mails. Now no one seems to mind.

It appears that sometime between the millennium and the present day the majority of Internet users have lowered their guard. We are willing to share tidbits of information on a daily basis, via Twitter, Facebook or one of the other countless social networking sites. The information we share seems harmless enough, so we share it, because it gives us a few minutes of pleasure to tap out a message and receive instant gratification.

The irony is that the information we share can be more dangerous now than ever. Take, for example, companies such as Virgin Airlines that have been known to use Facebook to keep tabs on their employees and have actually fired them over posts they made.

Advertisements on Facebook are displayed on a computer monitor in June last year. PHOTO: BLOOMBERG

What about location-based social networking sites, such as foursquare.com, a place where you broadcast your exact location to the users? These are dangerous because anyone on your list could easily be waiting for you to post about how you are enjoying your holiday abroad, and then know for sure that your house is empty and have a map directly to your front door.

### IS FACEBOOK EVIL?

Facebook came under fire recently after it made changes to its privacy settings. Users must now explicitly opt out if they wish for their information to be kept private, by default making most Facebook users' information public and sharing lots of it with third-party Web sites.

Your Facebook account can become much more private if you sift through the overly complex privacy settings and spend a good amount of time tweaking your profile. There are more than 50 different privacy buttons which require choosing from a total of more than 170 options. Even after this some information remains public, so the best way to limit access is to simply delete the information from Facebook.

It's clear that Facebook doesn't want you to have your profile set to private, and there is something awry when you consider that the US Constitution is more than a thousand words shorter than Facebook's privacy policy. Why? The core business model of social networking sites is to collect data from users and monetize it. Currently the largest chunk of revenue comes from supplying advertising based on this data, but in the future who knows how this data could be used. This is why Facebook wants your information public: to bring more people to the site, to provide more relevant advertising, and to make money from this advertising.

Shocking? Not particularly. If Facebook wants to share my film and music preferences with advertising companies, that's fine. If they wish to show relevant adverts to me, great. This is what Amazon, Google, YouTube and Yahoo started doing years ago. But the more Facebook tweaks its default settings to make previously private information public, the more users are closing down their accounts, something which has become known as "Facebook suicide."

One possible solution is to force large sites to add a button to their privacy sections that would say "What do you know about me?" and allow users to easily view and edit everything the site knows about them. But if the past is anything to go by, there will be a new privacy heretic next month for us to worry about, and Facebook will continue its practices in relative peace. If not, you can always commit Facebook suicide.

*Gareth Murfin is a freelance mobile developer www.garethmurfin.co.uk*