



LESSON LEARNED Elana Rivel makes sure all her passwords are more secure after cybercriminals hijacked her Facebook account.

Social insecurity

What millions of online users don't know can hurt them

Inside

State of the Net 2010

Page 25

7 things to stop doing now on Facebook

Page 26

Security software

Ratings page 29

Laptops, netbooks, and desktops

Ratings pages 32-37

Monitors

Ratings page 41

TWO OUT OF THREE online U.S. households use social networks such as Facebook and MySpace, nearly twice as many as a year ago, according to the latest CONSUMER REPORTS State of the Net survey.

But millions who use these services put themselves and their families at risk by exposing very sensitive personal information, according to the national survey of 2,000 online households conducted in January by the Consumer Reports National Research Center. Here are the details:

- Within the past year, 9 percent of social network users experienced some form of abuse, such as malware infections, scams, identity theft, or harassment.
- Many social network users are naïve about risks. Forty percent had posted their

full birth date, exposing them to identity theft. Twenty-six percent of Facebook users with children had potentially exposed them to predators by posting the children's photos and names. And in one of four households with a Facebook account, users weren't aware of or didn't choose to use the service's privacy controls.

- Among all computer users, established threats, such as spyware and phishing e-mail scams, persist at alarmingly high levels, and virus infections increased significantly since last year. Forty percent of online households surveyed reported that they had at least one virus infection in the past two years.

Those findings provide a reminder that it's still important to use the best anti-malware software available. (For Ratings

of the latest such software, see page 29.)

Overall, we estimate that cybercrime cost American consumers \$4.5 billion over the past two years. And it caused them to replace 2.1 million computers.

With social networks expanding the online opportunities for criminals, the price of cybercrime stands to grow even more. “We’re just at the beginning of seeing what the implications are for so much information being posted on social networks,” says Nicole Ozer, the technology and civil liberties policy director for the American Civil Liberties Union of Northern California.

But crime on social networks need not skyrocket. Protecting the vast majority of consumers doesn’t require developing any technology, as contending with viruses and spyware did during the past decade. It requires the networks themselves to keep improving their privacy practices and better educating users. (For tips on protecting yourself, see “7 Things to Stop Doing Now on Facebook,” on page 26).

When sharing goes too far

Being able to share your opinions, experiences, and photographs is the main reason for using a social network. But on Facebook, which is the largest service, with more than 400 million active users, some personal information you don’t protect can be read by anyone running a search

Cybercrime cost U.S. consumers \$4.5 billion and 2.1 million PCs.

engine, exposing you to a range of abuses.

“Criminals are opportunists,” says Charles Pavelites, a supervisory special agent at the Internet Crime Complaint Center, a partnership of the FBI, the National White Collar Crime Center, and the Bureau of Justice Assistance. Pavelites urges people to use the same caution when sharing sensitive data online as they would offline. “Wherever you have lots of people, they’ll see lots of opportunities,” he says. “How savvy the criminal is versus how savvy the social network is will determine how much happens. It’s a race, but we can’t say who will win.”

Natalie Connor, a software security industry public relations professional from Sydney, Australia, found that out the hard way. One morning last January, she got a message from a friend of hers on Facebook describing a potential match he’d found on the online dating service eHarmony.

She was 24, “a primary-school teacher

... and she’s using your picture,” he informed her. She was using Connor’s profile picture from her Facebook account. Connor contacted eHarmony, which soon took the photo down.

While it’s not certain whether using someone else’s photo that way is a crime, doing so could lead to civil action.

Connor said she had restricted access to her Facebook profile to just her friends. Yet she wasn’t entirely surprised at what happened, because her work has made her acutely aware of online threats.

“I thought I was safe online,” she says. “But in reality, how could I be?” In fact, it’s quite easy for other Facebook users, even those not on your friends list, to download photos you don’t protect.

For example, our reporter signed onto Facebook and accessed the unprotected portraits and profiles of numerous strangers, including information invaluable to criminals such as a mother’s maiden name and child’s middle name.

She was able to do it because Facebook had recognized that she and those strangers had friends in common, a relationship it calls “sharing a network.” Since, as our survey shows, many Facebook users don’t use privacy controls, someone who had only a handful of Facebook friends could conceivably access thousands of unprotected profiles.

State of the Net 2010

Internet threats continue at alarmingly high levels, costing consumers billions in damage. The number of virus attacks increased significantly since last year, affecting 40 percent of online U.S. households. Some households reported multiple problems.

| | SPAM | VIRUSES | SPYWARE | PHISHING |
|---------------------------|--|--|--|---|
| | 24 million households Experienced heavy spam | 16 million households Had serious problems in previous two years | 8 million households Had serious problems in past six months | 1 million households Lost money or had accounts misused |
| | Almost half of the households received suspicious e-mail offers in the past month. | 1.8 million households had to replace infected PCs in the past two years. | 617,000 households had to replace slow or impaired PCs. | There were 28,897 attacks in December 2009. Many involved financial e-mail scams. |
| National incidence | 1 in 3 had heavy levels of spam | 1 in 5 had serious problems | 1 in 11 had serious problems | 1 in 167 lost money |
| Trend | Down from last year | Up from last year | No change | No change |
| Total damage | NA | \$2.7 billion | \$1.2 billion | \$650 million |

Source: Consumer Reports National Research Center, based on a nationally representative survey, projected to the 82.3 million Internet-using households in the U.S. (source: eMarketer). The Anti-Phishing Working Group reported the number of phishing attacks.

Online con artists

Social networks provide a perfect environment for con artists. “People think they’re surrounded by their friends, and it’s easy to fool them,” says Kevin Haley, director of product management for Symantec, the security software company.

David Hiller, a freelance video journalist from Wayne, N.J., wasn’t so easily fooled by a Facebook chat message that appeared to come from Elana Rivel, a longtime friend from college. It claimed that she

and her husband had just been robbed at gunpoint in London and needed help.

Hiller responded by asking the sender for personal information to verify the sender’s authenticity—Rivel’s brother’s name. The sender was able to provide it, but Hiller quickly realized that the name was visible on Rivel’s Facebook profile. “I’m serious!” the next message to him said. But Hiller persisted, asking for the name of their college cafeteria. When the sender couldn’t provide that, Hiller

knew it was a scam.

Next, Hiller did exactly what security experts recommend in such circumstances: He attempted to reach Rivel via a separate e-mail address. But he soon realized that the same person had taken over that account, too. Finally, he called her workplace, only to learn that she was in Pennsylvania, not London.

Rivel, a synagogue consultant from the Philadelphia area, doesn’t know exactly how the scammers got into her Facebook

7 things to stop doing now on Facebook

► Using a weak password.

Avoid simple names or words you can find in a dictionary, even with numbers tacked on the end. Instead, mix upper- and lower-case letters, numbers, and symbols. A password should have at least eight characters. One good technique is to insert numbers or symbols in the middle of a word, such as this variant on the word “houses”: hO27usEs!

► Leaving your full birth date in your profile.

It’s an ideal target for identity thieves, who could use it to obtain more information about you and potentially gain access to your bank or credit card account. If you’ve already entered a birth date, go to your profile page and click on the

Info tab, then on Edit Information. Under the Basic Information section, choose to show only the month and day or no birthday at all.

► Overlooking useful privacy controls.

For almost everything in your Facebook profile, you can limit access to only your friends, friends of friends, or yourself. Restrict access to photos, birth date, religious views, and family information, among other things. You can give only certain people or groups access to items such as photos, or block particular people from seeing them. Consider leaving out contact info, such as phone number and address, since you probably don’t want anyone to have access to that information anyway.

► Posting your child’s name in a caption.

Don’t use a child’s name in photo tags or captions. If someone else does, delete it by clicking on Remove Tag. If your child isn’t on Facebook and someone includes his or her name in a caption, ask that person to remove the name.

► Mentioning that you’ll be away from home.

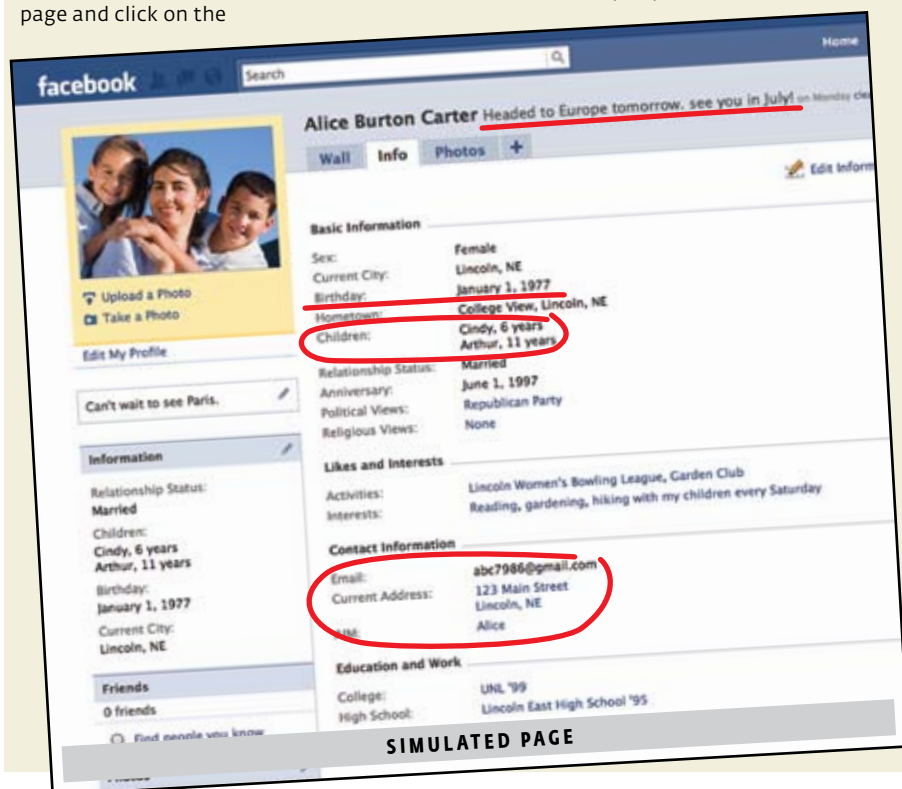
That’s like putting a “no one’s home” sign on your door. Wait until you get home to tell everyone how awesome your vacation was and be vague about the date of any trip.

► Letting search engines find you.

To help prevent strangers from accessing your page, go to the Search section of Facebook’s privacy controls and select Only Friends for Facebook search results. Be sure the box for public search results isn’t checked.

► Permitting youngsters to use Facebook unsupervised.

Facebook limits its members to ages 13 and over, but children younger than that do use it. If you have a young child or teenager on Facebook, the best way to provide oversight is to become one of their online friends. Use your e-mail address as the contact for their account so that you receive their notifications and monitor their activities. “What they think is nothing can actually be pretty serious,” says Charles Pavelites, a supervisory special agent at the Internet Crime Complaint Center. For example, a child who posts the comment “Mom will be home soon, I need to do the dishes” every day at the same time is revealing too much about the parents’ regular comings and goings.



account. But she's taking measures to avoid a recurrence. "The biggest thing I'm changing is being more mindful of my passwords," she says, noting that she now uses different passwords on all her sites. "I'm not going to stop using Facebook."

Being cautious in disclosing passwords can protect you from a variety of crimes. For example, scammers can send people an e-mail message, apparently from Facebook, telling them to click on an attachment to access a new password. Doing so installs software on their computer that grabs their user name and password.

Another scheme uses a hijacked social network account to send an online friend a Web link with an accompanying message, complete with the hijacked account's profile picture, which says something like, "Hey, watch yourself in this video!" Clicking on the link infects the recipient's computer with malware that the criminal uses to steal passwords.

To avoid becoming a victim, take the same precautions you would anywhere online: Don't respond to any message, no matter how official looking, that asks for a password or PIN. And don't click on links to videos you weren't expecting or share account information through online messages.

Apps that bite

Popular software applications (apps) available on Facebook let you take a quiz or play games like Farmville and Scrabble with others. Many social network users we surveyed were either confident that such apps are secure or hadn't given the subject much thought. But we project that 1.8 million computers were infected by apps obtained through a social network in the past year.

Kevin Johnson, a senior analyst at the security consulting firm InGuardians, recently showed how easy it can be to place an app on Facebook that does more than meets the eye. His app, KanyeWestify, imitates an infamous exchange between Kanye West and Taylor Swift during a music-awards show. The app posts a message on selected friends' walls in response to their status updates, telling them Beyoncé does whatever they did better. But Johnson says it also allowed him to grab the browsing history of anyone who signed up to use it, along with profile data of the user and friends. He says he has since removed the app's history-collecting capability.



STOLEN IDENTITY Natalie Connor was shocked to find someone else using her Facebook portrait as their own on a dating site.

Johnson isn't surprised that his deceptive app wasn't weeded out and removed from the network by Facebook. He says the company does a pretty good job of catching apps that download malicious software, adding, "But Facebook doesn't remove those that collect data, because it's within their terms of service."

A Facebook representative told our reporter that the company requires app developers to ask only for data that's needed for the application to function. Facebook says that it enforces the policy through

Many users don't realize that apps can pose risks.

spot checks and has disabled apps found in violation. It also says that no app can access the contact information or other sensitive information of any Facebook user without their permission.

When we tried to download an app, however, the service displayed a notice saying that the app can grab your profile information, photos, friends' info, and other content that is necessary for it to work. That could include a lot of sensitive information. For example, your profile can include your hometown and your children's names.

When you use an app, its developer can

collect non-contact information from all of your friends' Facebook accounts. But anyone can protect their data from apps they're not using by setting a privacy control.

Short but not sweet URLs

Compact versions of URLs (Web addresses), which online users can obtain from services that specialize in address shortening, are often used on social networks like Twitter to make it easier to post links.

No one can tell, just by looking at it, where a URL like bit.ly/16StNc will lead, so criminals sometimes use such addresses to mask malicious sites. (The one above, however, takes you to the home page of ConsumerReports.org.)

Last year, for example, some Twitter postings contained short URLs that linked to sites where people unwittingly downloaded malware called Koobface.

Things have improved since, says Morton Swimmer, a researcher for security software maker Trend Micro. "Short-URL providers have been very good at screening," he says. "I was skeptical at first, but none of my fears actually panned out in the long term."

But no safety net is perfect. To protect yourself further, we recommend that you use security software that includes a browser toolbar. That feature will alert you before you visit a risky site. Five security software suites we tested that have it are identified in the Ratings on page 29.