Prevent Online Identity Theft

HOW TO AVOID THE SCOURGE OF THE INTERNET. BY RUSSELL SHAW

Identity theft is as old as civilization, but the Internet has made the crime almost embarrassingly easy. If you don't take the proper precautions, criminals can obtain your name, your birth date, your driver's-license, credit-card, and social-security numbers—all for the purpose of obtaining money, goods, and services in your name.

Once you understand how online identity theft happens, you can take steps to ensure it doesn't happen to you. The problem arises because so much information about us as individuals is stored in commercial, private, and government databases. Take that state of affairs and combine it with the fact that it's almost become trivial for us to voluntarily provide information about ourselves in order to obtain goods and services over the Internet, and you have a opportunity ripe for fraud.

In their January 2004 report "National and State Trends in Fraud & Identity Theft, January-December 2003," the Federal Trade Commission announced that for the fourth year in a row, identity theft topped the list of consumer complaints, accounting for 42 percent of all complaints lodged in the FTC's Consumer Sentinel database. That number, which exceeded 560,000, was up 40 percent over 2002. And of that number, Internet-related complaints accounted for 55 percent of all fraud reports, up from 45 percent in 2002. The FTC found that identity theft was the leading fraud-related grievance, and it was a contributing factor in other scams.

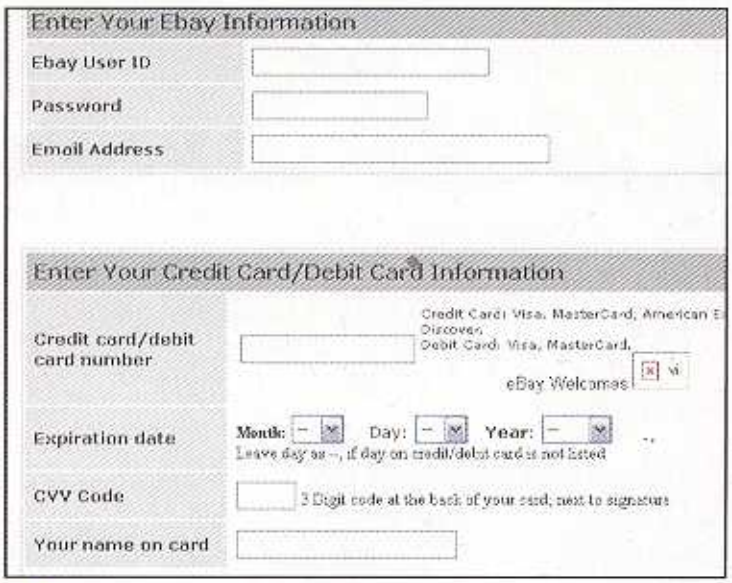
The consequences of identity theft can be enormous: Your credit could be smeared, you could lose out on that new job you applied for, or be denied for a home or car loan. Getting everything sorted out after the fact could takes hundreds of hours.

HOW CRIMINALS OPERATE

Although only an increasingly small percentage of online transactions are suspicious, criminals do use the Internet to commit identity theft, largely through an online version of the old confidence game. "Bogus emails that try to trick customers into giving out personal information," said Jana Monroe, Assistant Director of the Federal Bureau of Investigation's Cyber Division, "are the hottest and most troubling new scam on the Internet."

In what's known as a "phishing" scam, a thief produces an email that's designed to fool you into thinking it originated from a trusted source—your bank or credit-card company, for example. The email will attempt to trick you into revealing sensitive information about yourself by imploring you to click on what appears to be a link to a legitimate Website.

The ruse has been devastatingly effective. In May, 2004, the Gartner research firm noted that 19 percent of adult Internet users attacked by phishing scams clicked on the link presented in a phishing email. Of those attacked, 1.78 million adults supplied phishers with their financial or personal information.



This illegitimate Web page spoofed Ebay's credit-card entry form and was subsequently implicated in an identity-theft scheme.

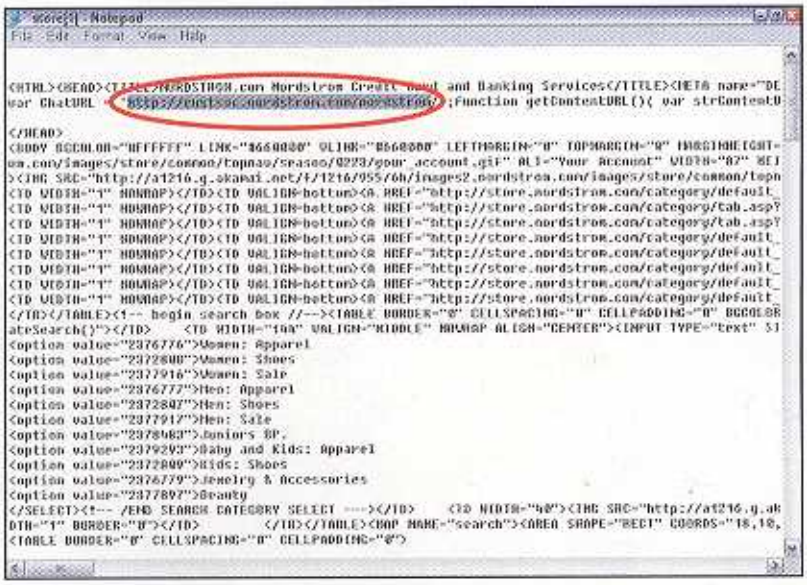
According to Gartner, phishing victims are almost three times more prone to identity-theft related fraud as other online consumers.

HOW PHISHING WORKS

For a phishing scheme to work, the perpetrator must make their e-mail—and later on, their Website—look perfectly legitimate. This is accomplished by a practice known as "spoofing." In an email spoof, email headers—information contained in every email message that documents the many computers it passed through before reaching its final destination—are forged to make it appear as though the message originated elsewhere.

In one spoof incident reported by Carnegie-Mellon University, email messages that appeared to originate with local system administrators went out to customers asking them to change their account passwords to new passwords contained within the message. The messages didn't originate with bona fide system administrators, of course, but from intruders trying to steal accounts.

In what's become a frighteningly more common scheme, a phisher will send you an official-looking email that appears to come from your bank, your favorite online retailer, or even your Internet service provider (ISP). The email claims that because of "internal accounting errors" or a recent "security breach," it is imperative that you update your personal information in order to prove your identity and/or keep your account open.



An examination of the source code for the Nordstrom Bank Website indicates that the site is legitimate and has not been spoofed.

Web-spoofing is email-spoofing's close relative. In a paper published by Princeton University computer-science professors Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach documented how a thief could design a fraudulent Website that exists between an end user and a legitimate Website. Upon coercing the victim to visit the legitimate site, the "fake" Website could intercept any information the user provided—such as a credit-card number—and forward it directly to the thief.

The FBI and the National White Collar Crime Center have teamed up to take on Internet fraud.

CONSIDER THE SOURCE

One of the easiest ways to avoid falling victim to such as scam is to never click on a link in an email that requests personal information. No legitimate company would make such a request, because they're very well aware of how these schemes operate.

If you've landed on a Website through some other means (a link on another site or even a listing in your Web-browser's Favorites menu) and you're still unsure it's legitimate, you can view the Web page's source code. If you're using Internet Explorer, click on the View menu and choose Source. A Notepad window will open displaying the programming statements used to create the page you're viewing. Click on the Edit menu, choose Find, and type the Web address you intended to visit. If you see this address displayed—without a suspicious look-alike address preceding it—you'll know the site is legit.

The U.S. Government's Federal Trade Commission also has some useful advice for avoiding online identity theft, including these nuggets:

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account,

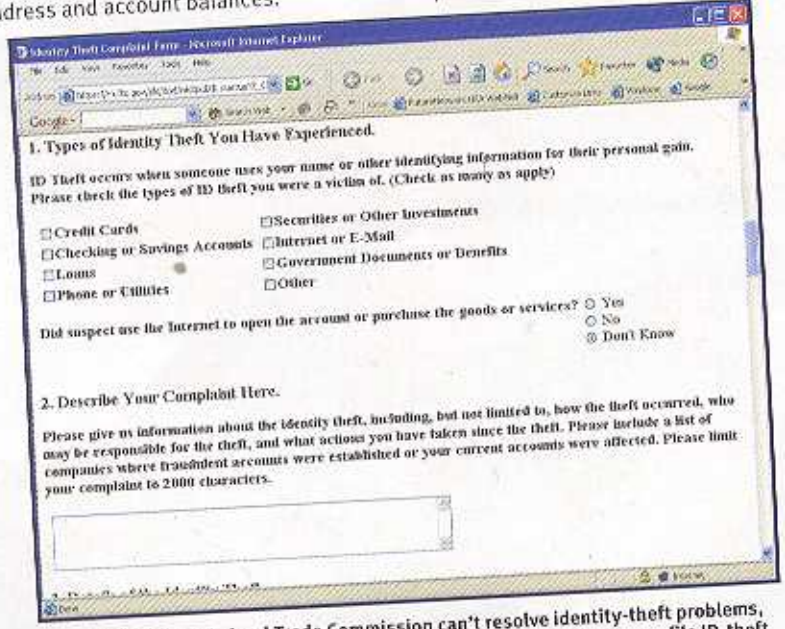
contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

All three major credit bureaus, including Equifax, offer subscription services that will monitor your credit history and alert you to changes.

- Review credit card and bank statements as soon as you receive them to determine if there are any unauthorized charges. If your statement is late by more than a few days, call your credit card company or bank to confirm your billing address and account balances.

- Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones, that can effectively reverse the damage, an that updates automatically.



Although the Federal Trade Commission can't resolve identity-theft problems, it does serve as the federal clearinghouse for such claims. You can file ID-theft claims on the agency's Website.

- A firewall helps make you invisibl on the Internet and blocks all communications from unauthoriz sources. It's especially important to run a firewall if you have a broadband connection.

- Your operating system may offer software "patches" to close hole the system that hackers or phish could exploit. For these fixes, ch Windows Update at windowsupd microsoft.com (no "www").

- Be cautious about opening any attachment or downloading any from emails you receive, regard of who sent them.

Utilities such as Ad-aware patrol your hard drive and look for spyware that might have been installed without your knowledge or permission.

To this advice, the non-profit Privacy Rights Clearinghouse adds the following suggestions:

- Install a firewall on your home computer to prevent hackers from obtaining personal identifying and financial data from your hard drive.
- Password-protect files that contain sensitive personal data, such as financial account information. Create passwords that combine six to eight numbers and letters in both upper and lower case.
- When shopping online, do business with companies that provide transaction security and that have strong privacy and security policies.
- Before disposing of your computer, remove data by using a strong "wipe" utility program, such as Erase Your Hard Drive (www.eraseyourharddrive.com). Do not rely on the "delete" function to remove files containing personal and/or sensitive information.

Online identity theft is as easy to avoid as it is easy to fall victim to. Unlike muggers or burglars, the criminals who steal identities online need your unwitting cooperation to pull off their heist. As long as you're reasonably vigilant, keep your computer protected with firewall, anti-virus, and anti-spyware software, and are always aware of where you are on the Web, you should be safe.

Some financial institution Websites offer forms where you can dispute charges caused by identity theft.

THE PERILS OF SPYWARE

One of the primary methods that thieves use to steal your identity online is install (or trick *you* into installing) spyware onto your computer. This is software used to monitor your actual computer activity. Sometimes, spyware is planted on a PC by a Website, or even by an individual who has access to the Internet-connected PC you are using.

Spyware works by recording the Websites and pages you have been to, and then monitoring your keystrokes while you were there (this particular form of spyware is known as a keylogger). Theoretically, spyware could use these capabilities to steal your credit card numbers and expiration dates, your passwords, and any number of other bits of confidential info.

The risk of encountering spyware becomes exponentially worse if you use public Internet terminals. In one well-known incident, a hacker surreptitiously installed spyware on Internet terminals in a New York-area Kinko's. Before he was caught, the crook captured more than four hundred user names and passwords and used them to access and even open bank accounts online.

There are two efficient ways to keep your identity from being hijacked by spyware:

- On your home or notebook PC, make sure that you have a software program that can examine your hard drive and look for spyware. Ad-aware is one of the best such utilities. At periodic intervals—daily, if you so choose—this program will look through your system, identify, and remove known adware and spyware.
- On public Internet terminals, the advice is obvious: never open a Website from the body of an email message, and never enter any specific financial information on any Website. The problem is the sheer number of anonymous users, who often are not even required to sign in. If you use online bill-pay and need to travel without a laptop computer, schedule the payment before you leave.

If you forget to do that and can't wait until you get home to pay your bills, use the PC in your hotel's business center. These computers typically require a valid ID and are protected by sign-in procedures. It's not a perfect solution, but it's better than nothing.