Technology (A Special Report) --- Stealing You: The latest on identity theft: How they do it -- and how you can protect yourself

By Andrea Chipman
1,591 words
26 April 2004
The Wall Street Journal
R8
English

THE HORROR STORIES are legendary. But for those who've experienced it, identity theft is all too real.

One misplaced credit-card application or indiscreet online purchase can produce a ruined credit record, thousands of dollars in expenses and months or years of precious time to clear the victim's name.

Cases range from opening credit-card or bank accounts in the victim's name, to taking over an existing account, to a mix of abuses including all of the above through wholesale assumption of a person's identity. According to a 2003 U.S. Federal Trade Commission report, some 9.9 million cases of identity theft were reported in the U.S. in the 12 months ended in April 2003, adding up to consumer losses of about $5 billion. The fraudsters find new victims and new ways of avoiding traps every day.

So what are the newest dangers, and how can you protect yourself? We asked a number of security and financial professionals in the U.S. and abroad about the most common forms of identity theft, and what consumers can do to avoid becoming a victim.

What are the newest scams?

In a trend known as phishing, criminal groups create a fake Web site that masquerades as the home page of a popular Internet provider or financial institution and tries to con personal information out of unsuspecting victims. Fraudsters send out e-mails directing the recipients to the spoof Web site, where the visitors find instructions to update or confirm records by entering their bank and credit-card information, personal identification numbers and other confidential data.

Fraud investigators say the phishing phenomenon has taken off in just the past few months. A site pretending to be that of PayPal, the online payment service, was used in a scam several months ago. Other recent scams have posed as home pages of Internet provider AOL and the Federal Deposit Insurance Corp., to name just a couple, government and financial experts say. The danger of phishing is that the sites look disconcertingly real, investigators add. And Internet users, accustomed to the ease of completing bank business or tax-return preparation with just a click of the mouse, can be easy marks.

Part of the problem was attributed to a flaw in Microsoft Corp.'s Internet Explorer program, which enabled criminals to hide the actual Internet address of a spoof page and thus fool Internet

users who were unaware they were clicking on a phony site. Microsoft has since patched the flaw, making it easier for vigilant users to see the Web address of a site on which they are clicking. But inattentive or inexperienced Internet surfers remain vulnerable to phishing scams.

"Criminals are practicing crimes on the Internet that they were always practicing face-to-face," says Graham Dowling, an industry liaison officer with Britain's National Hi-Tech Crime Unit. Both consumers and companies need to be more vigilant about verifying their counterparts in Internet transactions, he says.

Fortunately, avoiding this particular kind of trap is relatively easy: Don't take the bait.

"If you are dealing with financial institutions, they will never ask you directly for information that is pertinent and personal about your account -- they already know they have that information," says Mr. Dowling. "They will only ask you for certain parts" of your personal information.

Make sure you are entering a genuine site by typing out a Web address that most people should have stored if they have regular dealings with the bank or payment service. Many businesses that have been targets of spoof sites have posted warnings on their home pages, so always check, and above all, never click on an unsolicited link.

What about viruses?

Internet users have more to fear than just phishing expeditions, say information-technology experts. Spyware, a form of software that is frequently hidden in pop-up advertising and other unsolicited Internet message attachments, is increasingly being used to invade the hard drives of computer users, says Patrick Kolla, director of Safer Networking Ltd., a software company based in Bochum, Germany.

Some Web advertising companies use spyware legitimately as a tracking device to obtain information about your buying habits and the sites you visit, in an effort to serve up tailored advertisements. But another form of spyware, known as a key logger, acts as a form of Trojan horse, stealing serial numbers for software, computer games and operating systems to gain control over the machine or gain access to e-mail accounts to launch Internet attacks. Key loggers also have the potential to pick up any other personal information or account numbers that are stored on a computer system, although there have been few reported cases of key-logger programs being used to commit traditional forms of identity theft, Mr. Kolla says. Many complaints have involved ex-spouses using such programs to read the e-mails of their former partners, he adds.

Simple vigilance and common sense are key to avoiding spyware problems. Users should remain cautious about opening e-mail attachments, the biggest gateway for key-logger spyware. Also avoid opening pop-up ads or clicking on special promotions that appear on your screen, Mr. Kolla says, adding that if an offer seems too good to be true, it probably is. Be cautious about ordering goods on the Internet, and always make sure that the vendor is using a secure browser.

Keeping operating systems and antivirus and firewall systems up to date makes it harder for spyware to get a foothold in your system. A number of antivirus-software makers also now provide programs that can detect many different kinds of spyware, although they have varying degrees of effectiveness. Mr. Kolla's organization, found at Safer-Networking.org, produces and configures antispyware systems for corporate computer networks and offers its own program, Spybot, free to individual computer users. Other highly rated programs include PestPatrol from

PestPatrol Inc., Carlisle, Pa., SpywareEliminator from Aluria Software LLC, Lake Mary, Fla., and Ad-aware from Lavasoft, a unit of Nicolas Stark Computing AB in Sweden.

What should you do if you suspect you are a victim?

The first step you should take if you think you have been a victim of identity theft is to contact a credit bureau and put a fraud alert on your accounts. In the U.S. there are three main credit agencies -- Experian, a unit of U.K.-based retail and business service group GUS PLC; Equifax Inc., Atlanta, and Trans Union LLC, Chicago. A call to one of these will automatically result in a notification to the other two.

Next, fill out an ID Theft Affidavit, a document developed by the Federal Trade Commission that reports information about yourself and the theft. The affidavit also includes a Fraudulent Account Statement, where you describe fraudulent accounts opened in your name. Both should be sent to each company you have an affected account with. The FTC counsels that you use a separate account statement for each company or bank you need to write to. Always send copies, not originals, of any supporting documents, and use certified mail with return receipt requested. Keep a meticulous record of all correspondence with credit agencies, law enforcement and companies, experts advise.

Third, file a police report if at all possible. Some jurisdictions refuse to take reports. Some states don't have laws on the books pertaining to identity theft, and some local police can be reluctant to take a report for a fraud crime if the victim can't prove it took place in their jurisdiction. Be persistent, the FTC advises, and remind local authorities that credit bureaus will only take action against fraudulent accounts and debts if they receive a police report. Contact state police if necessary.

They got me. How can I repair the damage?

A program was launched by Citigroup Inc. in October for Citigroup credit-card holders who have been victims of identity theft or large-scale credit-card fraud. The New York-based bank provides a representative to personally walk the customer through such steps as closing unauthorized accounts or accounts that have been tampered with, and filing fraud alerts with credit bureaus. The representative can also help close accounts with other creditors and negotiate with credit bureaus. The Financial Services Roundtable, a Washington-based network of large financial institutions, is considering launching a similar service later this year.

The FTC maintains an Identity Theft Data Clearinghouse, the U.S. government's main database on identity fraud, and can provide information to victims. The clearinghouse Web site, www.Consumer.gov/IDTheft, allows victims to download two guides on how to deal with identity theft. It also contains links to the ID Theft Affidavit, as well as Web addresses and telephone numbers for the three main credit agencies and the Fraud Victims Assistance Division, where victims can report theft. The clearinghouse can also be reached toll-free at 1-877-438-4338.

Visa USA Inc., San Francisco, has set up its own service to assist identity-theft victims in partnership with the nonprofit consumer watchdog Call for Action Inc., Bethesda, Md. Callers to the venture's 1-866-ID-HOTLINE (1-866-434-6854) can receive confidential counseling, and additional information is available at CallForAction.org.

Ms. Chipman is a reporter for Dow Jones Newswires in London. She can be reached at andrea.chipman@dowjones.com