Web Can Be Avenue For Identity Theft

Don't Be Seen Napping

Anti-fraud specialists say online users should review accounts often

BY DONNA HOWELL
INVESTOR'S BUSINESS DAILY

Need a reminder why you should check your bank and credit statements?

Here's one: Imagine your worst financial nightmare. Now imagine that multiplied tens of thousands of times.

That's how a prosecutor describes the biggest identity scam in U.S. history, busted last month. It compromised the financial lives of up to 30,000 people. Some victims found their bank accounts drained, their credit ruined. The total take was millions of dollars.

The case provokes a question: How on earth can people protect their good names — and money? The truth is, there's no fail-safe way to guard your identity. But a little planning can cut the risk.

In the recent case, a help desk worker at a financial data firm allegedly sold passwords to consumer credit report databases. Information there helped crooks hijack people's identities, pry open their bank accounts and get new credit in their names.

It "shows how sophisticated these identity theft networks have become," said James Vaules, chief executive at National Fraud Center Inc., a risk management firm in Horsham, Pa. "Two, three or five years ago, identity theft was someone stealing your wallet or getting into your trash can."

The identity thieves used technology to do their deeds. But technology can also help consumers fight back. Regularly reviewing one's accounts online can catch trouble early.

Fraud fighters suggest checking your credit history for unusual activity at least annually. Get a copy online at the Web sites of the three major credit-reporting outfits: Equifax (equifax.com), Experian (experian.com) and TransUnion (tuc.com). Consumers can also dispute information online.

Credit reports can cost several dollars apiece. But they may be free to those recently denied credit, unemployed or who suspect fraud. A person can also ask that a security flag be temporarily added to his credit report. It tells potential creditors to take extra steps to verify identity before granting new credit.

The credit-reporting firms' sites also sell ongoing vigilance to consumers who want to keep close tabs on their accounts. The services run up to about $80 a year.

Don't Write Passwords

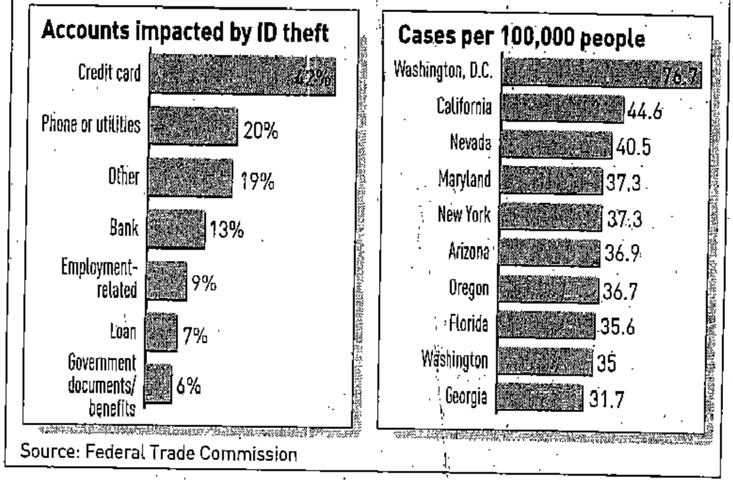
"The credit bureaus have alert services where you're notified if a new request has been made against your account," said Vaules. "Do you have to pay for it? Yes. But it's probably not a bad idea."

A separate service at privacyguard.com — also for a fee — can periodically check all three major credit-reporting firms, as well as driver's license and Social Security data.

Security pros warn to fiercely guard your personal data online. They also recommend computer protections, such as firewalls, intrusion detection and anti-virus software.

Not-So-Private Lives

When identities are stolen, credit card accounts get most of the abuse. California has the most cases of ID theft, but Washington, D.C., leads on a per-capita basis



Source: Federal Trade Commission

Another tip is to avoid writing down your passwords or keeping them in any unencrypted file on your computer. Also, look for a padlock icon at the bottom of your Web browser screen (or an "https:" starting the Web address) before submitting confidential data. It shows that a secure online connection is present.

E-mail scams are another threat. Watch out if you get an e-mail that appears to be from your Internet service provider and asks you to update your account information or credit card. It could be fraudulent.

You should also be careful about typing private account numbers and passwords on public-use computers, Vaules says. They're a quickly growing source of identity theft.

Spyware Penetrates Firewalls

"When you go to a computer center that has public access — at airports, hotels, Internet cafes or universities — you need to be aware the fraudsters have targeted those type of facilities with keystroke recorders," he said. "They record activity during the day and send it off to another computer. So if you're conducting business on these machines, you need to be careful."

Keystroke-logging programs may reach your computer through the Internet, says John Pescatore, research director for Internet security at analysis firm Gartner Inc.

"Even a personal firewall will let through what's called spyware," he said. "This is a huge problem. I think in the future it's going to be a big source of identity theft."

Spyware is largely any hidden feature of a piece of software that reports back data about the user to a Web site. Pescatre suggests using a free program called Ad-aware — from Lavasoft (lavasoftusa.com) — to find and delete spyware.

Even if you take steps to keep your information safe, you're taking a risk any time you give out personal data. That's why safer practices at businesses are also needed, fraud specialists say. The legal system may remedy matters, some say.

"Historically, consumers have not sued the keepers of sensitive personal financial data on a wide scale," said Toby Bishop, president of the Association of Certified Fraud Examiners. "It is inevitable that there will be major lawsuits against companies that keep such senstive information without adequate protections in place to prevent the data getting into the hands of the fraudsters."