Security
May 5, 2009 4:00 AM PDT

FAQ: Demystifying ID fraud

by Elinor Mills

Every time I use my credit card online I suffer a momentary feeling of angst, even though I know that **it's still safer than handing my card over to an unscrupulous waiter**. The impersonal nature of the Internet and the perception that I lose control of my data after I hit "submit" contributes to this lack of sense of security.

Also contributing to this paranoid feeling are all the reports of phishing scams, including IRS and **tax-related scams**; data breaches at **retailers like TJX**, where more than 45 million accounts were exposed; and payment processors like **RBS WorldPay**, where stolen data led to cloned cards and ATM withdrawals last year.

This all got me to wondering exactly how the data gets from my credit card or keyboard ends up as money in the pockets of criminals.

How does the data get stolen from my computer?
There are many ways sensitive data can be pried out of computer users. In a typical social-engineering phishing attack, a consumer opens an e-mail that looks like it was sent by the consumer's bank, Amazon, PayPal, or some other trusted source. With a bogus excuse, such as suggesting there was a security incident and the user needs to verify his or her account details, the e-mail will prompt the recipient to provide username and password via a link to a Web site that looks legitimate but isn't. The consumer enters the information and continues on, not knowing that the data is now being sent to criminals.

In other cases, criminals create fake e-commerce Web sites
where consumers provide their credit card information to pay for a product that will never arrive. Attackers also have ways of rendering legitimate Web sites risky by

injecting malicious code into the Web sites with cross-site scripting, SQL injection, and clickjacking attacks. Such attacks, typically invisible to the consumer, can be used to steal data that a consumer types in.

Other attacks are accomplished by getting spyware onto a victim's computer. For instance, attackers can distribute a worm via an e-mail attachment that downloads a keystroke logger onto the recipient's computer when it is opened. Attackers also can create programs that exploit unpatched holes in Windows or holes in a browser that haven't been fixed and download keyloggers onto computers. The keyloggers can be written to send data to a remote server every time the computer user types a password or social security number, for example.

If I don't use my credit or debit card on the Internet, how does the data get stolen?

Attackers can steal data by planting a skimming device that reads the magnetic-stripe data from the card when a user slides it through a payment card reader at a register or using a skimmer on an ATM machine combined with a video camera that records the PIN when someone is making a transaction. The magnetic-stripe data includes name, credit card number, and expiration date.

Attackers can steal more people's payment card data at a time by hacking into a retail firm or payment processor's computer network. In the TJX incident, experts believe attackers made their way into the company's system by first gaining access through a wireless regional hub for the company's store controllers, which handle the point-of-sale system. Attackers also can grab unencrypted PINs from bank systems during the authorization process using specially crafted malware that scrapes the data from the memory of the bank's computer, **according to Wired**. Or attackers can trick a misconfigured hardware security module, which decrypts and re-encrypts PINs as they make their way across various bank networks, into revealing the encryption key.

What do the criminals do with the data when they get it?

Cybercriminals tend to have specialties. The data thieves, also called "harvesters," sell it to brokers who either use the data themselves, hire others to do the leg work to

withdraw the money, or sell it to others via IRC channels, private peer-to-peer networks, carder sites, and other **organized underground marketplaces**.

Often, the data is sold with a money-back guarantee in the event that the cards are found to have been reported as stolen or if the data is incorrect. Brokers have a number of ways of verifying cards. They can break into an e-commerce Web site and process small transactions on the card with a payment processor to see if the transactions go through. Or they can use the card data to make a $1 donation to a charity.

Once the data is verified, the criminals can turn it into cash by either moving the money from the victim's account to an account they control, wiring themselves the money, creating counterfeit checks, or even just withdrawing small amounts (under $50) on a regular basis that may not get noticed by the cardholder.

Many of the criminals are located outside of the data's country of origin and will need to be able to either transfer funds or make international purchases without alerting the authorities. To do this, criminals have elaborate schemes using middlemen, also known as "drops." For instance, criminals will advertise work-from-home jobs in the U.S over the Internet and by e-mail. The drop is merely asked to provide a local address or bank account and when money or goods arrive, they are instructed to transfer it on to a foreign address. The criminal then takes over the bank or credit card account for which data was stolen, and changes the address or bank account to that of the middleman.

"The countries where re-shipping happens include Nigeria, where you can't easily buy consumer goods. This is a way for them to get goods," said Dave Ostertag, global investigations manager at Verizon Business who used to be a chief investigator at Discover Card. "This fraud stocks the shelves of a store in another country."

An estimated 70 percent of the online identity fraud activity is related to organized crime, Ostertag said. In the U.S., street gangs can make more money off mortgage fraud than they can selling drugs, he added.

The criminals also can make blank plastic cards that are encoded with the stolen magnetic-stripe data. Often, cards are produced in one country and shipped back to the country where the account is located. The cards then can be used by "runners" to make withdrawals from ATM machines if the PIN codes are known.

Criminals have been known to use private databases to get more complete information on victims, such as address, date of birth, and even social security number. For instance, the **U.S. Postal Service says someone accessed LexisNexis** and Investigative Professionals databases without authorization and used personally identifiable information from there to obtain fraudulent credit cards.

Bank Name	Country	Balance	Price
Bank of America (BOA)	USA	...	Sold
Amsouth Bank	USA	$16,040	€700
Washington Mutual Bank(WAMU)	USA	$14,400	€600
Washington Mutual Bank(WAMU)	USA, Multi-currency acct.	$7,950 + £2,612	€500
Washington Mutual Bank(WAMU)	USA	...	Sold
MBNA America Bank	USA	$22,003	€1,500
BANCO BRADESCO S.A.	BRAZIL, Dollar Account	$13,451	€650
CITIBANK	UK, GBP Account	£10,044	€850
NatWest	UK, GBP Account	£12,000	€1000
BNP Paribas Bank	France, Euro Account	€30,792	€2200
Caja de Ahorros de Galicia	Spain, Euro Account	€23,200	€1200
Caja de Ahorros de Galicia	Spain, Euro Account	€7,846	€500
Banc Sabadell	Spain, Euro Account	€25,663	€1450

Screenshot of price list for stolen credit card numbers and available balance amounts discovered on the Web by McAfee Avert Labs.
(Credit: **McAfee Avert Labs**)

How much is the data worth?

There is so much stolen magnetic-stripe data available on the underground markets that prices for it have dropped from between $10 and $16 per record in mid-2007 to less than 50 cents per record today, according to the **2009 Data Breach Investigations Report (PDF)** from Verizon Business. Those price tags go up when the PIN is available and cash can be withdrawn directly from a victim's account.

The value of a card is determined by a combination of factors. Cards from the U.S. and Europe fetch higher prices, as do cards with more available credit or balance, those with additional information such as PIN or home address, and those that have been verified.

Credit card data can range in price from 6 cents for bulk quantities to $30, while bank account credentials range from $10 to $1,000, according to a Symantec Internet Security Threat Report **released last month**. Most of the stolen credit card data for sale is from the U.S., the report found.

Is the consumer liable for any fraudulent charges?
While credit card fraud typically has a zero-liability policy for consumers, the burden of proving fraud is on the consumer when it involves a debit card.

How big a problem is online identity fraud?
The latest Consumer Reports survey found that over the past two years 1 out of 13 Americans provided personal data to phishers, 1 in 12 had serious problems with spyware, 1 in 7 lost money to online fraud or had computer virus problems, and about 1.7 million were victims of identity fraud, the San Francisco Chronicle **reported on Monday**.

A **report from Javelin Research (PDF)** places the number of identity fraud victims in the U.S. at 10 million in 2008. Identity fraud rose 22 percent last year from the year before to the highest level since 2004, the report said. Meanwhile, online theft and data breaches each represented 11 percent of the known identity fraud incidents, compared to 43 percent for lost or stolen wallets and 19 percent that occurred during a transaction.

Payment card breaches represented 80 percent of the 90 reported breaches last year, and payment card data represented 98 percent of all records compromised, according to

the report from **Verizon Business**.

Between January and December 2008, consumer complaint database Consumer Sentinel Network received more than 1.2 million consumer complaints, according to a **report released by the U.S. Federal Trade Commission (PDF)** in February. Of those, 52 percent were fraud complaints and 26 percent related specifically to identity theft.

Complaints of online crime hit a record high last year and total dollar loss linked to online fraud was $265 million, according to **a report released in March** by The Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center. The third most common fraud complaint was credit or debit card fraud, representing 9 percent, preceded by non-delivery of merchandise or payment at 33 percent, and Internet auction fraud, representing more than 25 percent.

What can consumers do to protect themselves?

To protect against online identity fraud, consumers (who use Windows) should sign up for regular automatic Microsoft software updates, use the latest browser versions with enhanced security features, and keep their antivirus and other security software up-to-date. To avoid phishing and other malicious sites when Web surfing, there are a number of programs, including McAfee Site Advisor and AVG LinkScanner.

McAfee also recently launched the **McAfee Cybercrime Response Unit**, where people can go if they suspect they have become a victim of cybercrime or identity fraud. The site has a free Windows-based scanner that can give an indication of how likely the consumer is to have been victimized, as well as specific steps to take in the case of identity fraud. These include changing account passwords and PINs, placing a fraud alert on credit reports, and reporting the crime to authorities.

The **FTC's Identity Theft Site**, the **Identity Theft Resource Center**, and The Privacy Rights Clearinghouse's **Identity Theft Victim's Guide** have more information.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Privacy & data protection**, **Vulnerabilities & attacks**

Tags: **identity fraud**, **ID fraud**, **phishing**, **data breaches**, **cyber crime**

Share: Digg Del.icio.us Reddit Yahoo! Buzz Facebook

Related

From CNET

Survey: Credit card fraud a top concern in U.S. as economy melts

The Dancing Woz eliminated--Conficker to blame?

Symantec investigating customer credit card data theft

From around the web

Steps to Prevent Identity Theft, and Wha... The New York Times

Glut of Stolen Banking Data Trims Profit... Washington Post Blogs - Securi...

More related posts powered by Sphere