PHYS.ORG

Latest data breach strikes at financial security

June 11 2011, By PALLAVI GOGOI , AP Business Writer

In this Apri; 30, 2009 file photo, a sign for Citibank is shown at Citigroup headquarters in New York. For the 200,000 people with Citigroup credit cards who had their names, account numbers and email addresses stolen by hackers, the breach is mostly a nuisance. (AP Photo/Mark Lennihan, file)

(AP) -- Citigroup's disclosure that the names, account numbers and email addresses of 200,000 of its credit card customers were stolen strikes at the core of modern-day financial life - the ways people buy groceries and pay the power bill.

It's only the latest major data breach. In just the past three months, hackers have penetrated 100 million Sony PlayStation accounts, the networks of Lockheed Martin and the customer email databases of a company that does marketing for Best Buy and Target.

But half of all Americans, 154 million people, have a credit card. The Citi attack is a reminder that the technology used to protect their information was built by humans, security analyst Jacob Jegher notes - and it can be breached by humans, too.

"People rely on the safety net of a bank to take care of their information," says Jegher, a senior analyst at Celent, a research firm that focuses on information technology in the financial industry. "Unfortunately, that net has a lot of holes."

Citi says all of the customers whose information was stolen will receive a notification letter, and most of them will get a new card, although it has declined to say exactly how many. The bank says its enforcement division and authorities are investigating.

The victims will have to endure the hassle of updating the credit card numbers on any number of online accounts, but they probably won't lose any money. For one thing, federal laws protect credit card customers from fraud beyond $50, and in most cases, the bank that issues the card will cover up to that amount.

And the Citi hackers didn't get to the three-digit numbers that appear on the backs of credit cards, a security feature known as the CVV code. That means the hackers, or whoever they might sell the information to, would have trouble making direct charges.

The danger is that someone might use the information that was compromised to mount a sophisticated "phishing" attack, in which criminals send out convincingly designed emails pretending to be from the bank and gain access to account information.

The relatively small number of accounts taken from Citi, which has 21 million credit card customers in North America, suggests the hackers used spyware that captured the data of customers who logged in to its website to conduct online banking, one expert says.

"The thing in the Citi case which is good is they detected it quickly and shut it down," says Dave Jevans, chairman of security firm IronKey Inc. and chairman of an anti-phishing nonprofit group made up of 2,000 government agencies and companies, including Citi.

"They've got systems that are going to look at the data leaving the network and are able to see that somebody's sending information out," he adds. Banks are ahead of most other industries in this regard, he explains, and other businesses will have to catch up.

CVV codes can't be stored with a simple magnetic swipe of a credit card, and the businesses that process payments are not allowed to store the codes after a transaction, so they provide another defense against fraud.

Deloitte, the audit and consulting firm, said in a report last year that security threats to customer account and other information were on the rise. The good news: Companies are taking notice.

The number of companies that said they didn't spend enough on security fell to 36 percent in 2010 from 56 percent the year before. The survey found that 67 percent of U.S. banks are making encryption, a process to protect digital information, a top initiative.

Still, Deloitte also reported that of all nations, the United States had the most financial institutions that were still "catching up" on security, as opposed to being ready or "on plan." And the number of high-profile attacks in recent weeks is frightening.

Tyler Lesthaeghe, a senior at Iowa State University, got a call from Citi on a Saturday morning two weeks ago and was told that his credit card number had been stolen. No fraudulent charges were made, and he received a new card two days later.

Lesthaeghe's case appears unrelated to the attack that Citi disclosed Thursday. Credit card information can be stolen in ways other than a direct attack on the bank, from sophisticated attacks elsewhere in the network that processes card payments to a corrupt waiter who writes down the numbers.

He says he expects this sort of thing to happen more often in the Internet age and checks his credit report regularly and his account statements every month.

"You have to be diligent about it," he says. "It seems like large amounts of credit card numbers are getting stolen. It's kind of scary to hear that."

Security experts say there are several steps you can take to protect yourself:

-Check your credit report regularly to make sure stolen information isn't being used to open new accounts. That scenario is unlikely in the Citi case because the hackers didn't get enough information, but it's good to check anyway.

"Where consumers have to be very concerned is when information like their date of birth, their Social Security number or their mother's maiden name is breached," says Tom Osherwitz, chief privacy officer at ID Analytics.

Everyone is entitled to a free annual report from each of the three major credit reporting companies, Experian, Equifax and TransUnion. Those reports can be accessed at annualcreditreport.com, which also explains how to set fraud alerts. Ordering one every few months and rotating the companies essentially allows you to check your credit regularly for free.

-Vary the user names and passwords on your online accounts, and make sure to change any user names and passwords that match those in an account that may have been hacked.

-Third-party services will monitor accounts established in your name and alert you to something suspicious. If you decide to pay for one, make sure it covers all three credit bureaus and tells you about all activity in a timely manner. Otherwise, it's not worth the money.

-If you are the victim of identify theft, report it to the authorities. Details on how to do that are at onguardonline.gov, a security site developed by several federal agencies.

Citation: Latest data breach strikes at financial security (2011, June 11) retrieved 20 April 2024 from https://phys.org/news/2011-06-latest-breach-financial.html