Banks, credit-card issuers warn of e-mail breach
By LAURA GREEN

Palm Beach Post Staff Writer

Updated: 6:21 p.m. Monday, April 4, 2011
Posted: 6:14 p.m. Monday, April 4, 2011

Check your in-box. You may be one of millions of Americans who have received a message warning that your e-mail address was captured by hackers.

Large companies such as Chase, Citi and Best Buy said during the weekend that hackers may have learned the e-mail addresses of their customers because of a security breach at Epsilon, a Dallas-based company that manages e-mail communications.

Corporations that use Epsilon's services have started warning customers to expect fraudulent e-mails that try to coax account log-in information from them.

This breach may be more widespread but it is likely less damaging than other cases when customers' credit card numbers, for example, were hacked, said Roy Levow, Florida Atlantic University computer science professor.

The hackers' initial target, e-mail addresses, are relatively harmless. But the bigger threat is that those addresses will allow fraudsters masquerading as legitimate corporations to lure customers to inadvertently share their financial information.

"Knowing where you have accounts does offer more opportunity because it can create an impression of validity that anonymous e-mail or guessing won't do," Levow said.

Epsilon has a number of financial institutions as clients, so consumers should carefully read any messages that appear to come from your bank.


The College Board, the not-for-profit organization that runs the SATs, also warned that a hacker may have obtained student e-mail addresses.

David Jevans, chairman and founder of the non-profit Anti-Phishing Working Group, said criminals have been moving away from indiscriminate phishing toward more intelligent attacks known as "spear phishing," which rely on having more intimate knowledge of the victims.

"You're not going to see typical phishing where 90 percent of it ends up in spam traps and is easily detected. This is going to be highly targeted," he added.
It’s also a standard tactic among online fraudsters to send e-mails to random people, purporting to be from a large bank and asking them to login in at a site that looks like the bank’s site. Instead, the fraudulent site captures their login information and uses it to access the real account.

Walt Disney Co.’s travel subsidiary, Disney Destinations, sent e-mails warning customers on Sunday. Hotel chain Marriott International Inc. issued a similar warning.

To be safe, Levow urges consumers to look carefully at any links embedded in e-mails that appear to be companies with which they do business. Hover your arrow over the link in the e-mail and the address will show up, Levow said. If the web address ends in ru, for example, you know the website is based in Russia, Levow said.

"You want to be very sure the website is the one you know belongs to that company," he said. "Most of the phishing exploits are not very sophisticated about the URLs they use."

The first line of defense, Levow said, is to have good security software on your computer.

Epsilon said Friday that its system had been breached, exposing e-mail addresses and customer names but no other personal information.

Epsilon, a unit of Alliance Data Systems Corp., sends more than 40 billion e-mails annually and has more than 2,500 clients.

Jill Kocher in Crystal Lake, Ill., said she got at least five e-mailed warnings, including from U.S. Bank, Best Buy and New York & Co.

Because she works for Groupon, an Internet coupon company, she feels savvy enough to avoid any phishing come-ons, but she’s concerned for those who aren’t.

"U.S. Bank sends you an e-mail and it looks legit and you cough up the information, and now you're in big trouble," Kocher said. "It sure does sound like a big increase in fraud, just waiting to happen."

*The Associated Press contributed to this story.*