



Monday, November 19, 2007

'Vishing' is newest card scam Consumers bilked into revealing data

By Shelly Whitehead
Post staff reporter

"Please notice that your VISA card is now disabled and you will not be able to use it. ... This is a security measure made by your bank. ..."

That's the kind of e-mail message that gets your attention. And some of those who recently received it probably did just as instructed and called the provided toll-free number to re-activate their credit cards. The problem is their cards were never de-activated in the first place. And if they called in and keyed in their card numbers, they opened their accounts up to a world of criminals.

That e-mail and many others just like it represent one of the latest trends in computer-based scams known as "vishing," short for voice phishing.

Like e-mail phishing operations, vishing also works by tricking people into handing over confidential financial account information. But instead of directing people to bogus Web sites, vishing scams instruct victims to call a phony company phone number, where they are typically directed to enter their identification numbers to rectify some fictitious problem with their accounts.

Vishing scams began cropping up after word got out about traditional phishing scams, in which e-mail is used to lure the unsuspecting into giving up financial information, and consumers became far less likely to take their bait. But computer crime experts, like Capt. Jack Prindle of the Boone County Sheriff's Department, say consumers aren't as wary of entering credit card information into a telephone keypad.

"The bad guys needed a different wrinkle, so now the bad guys get you to call a machine," Prindle said. "For people with a phobia about giving their credit card information on the Internet, this allows them to make contact with them and steal their credit card information."

Experts say some vishing scams even skip e-mail entirely and work their arks entirely by telephone. By using Voice over Internet Protocol technology, scammers know they can hide the source of the call. Some vishers have even learned how to misrepresent the call's source in the victim's caller ID display as that of a financial institution.

Last year, many vishing scams targeted customers of eBay's online payment service, PayPal. But this year, experts say voice phishing has moved beyond large credit card and online payment company customers to clients of smaller financial institutions.

And the purveyors of such scams seem to stop at nothing to gain and then abuse your trust. For instance, Prindle recently received an e-mail from an organization claiming that a "new security system to make Credit Union accounts more secure and safe" had been initiated on his account.

The electronic message said Prindle's credit card had to be deactivated to launch the new system and it instructed Prindle to call a provided phone number to re-activate his account. Prindle investigated the source of the e-mail and quickly confirmed it

KEEP ALERT

Phishing and vishing prevention tips:

Be wary of all solicitations for account information.

The Federal Trade Commission advises that consumers contact their financial institutions using only the phone numbers or Web site addresses provided independently through the actual card or on the monthly statement. Never use contact information provided in e-mails.

Install and regularly update anti-virus software, firewall programs, spyware and e-mail filters.

Update Internet browsers and apply security patches.

Each month check online account, credit and debit card and bank account information for accuracy.

Avoid e-mails requesting financial information or threatening account termination.

To ensure you're on a secure Web server, your browser's address should begin "https://" NOT "http://"

To report suspicious e-mail, fill out a complaint form at the Internet Crime Complaint Center at www.ic3.gov.

ADVERTISEMENT

[Advertise Here](#)

[Ads by Google](#)

[Identity Theft Protection](#)

Opt out of marketing lists that identity thieves can target - Free!
www.proquo.com

[Equifax - Official Site](#)

Protect Against ID Theft & Credit Fraud w/ Equifax Credit Monitoring
www.equifax.com

[419 Scam Warning](#)

These Programs Are Absolute Scams I Will Show You The Ones That Work
IGotScammed37Times.com

was phony.

Perhaps more interesting is the lengths that Prindle found those behind the scam had gone to hide their identity and bypass the spam-blocking software now used on most e-mail accounts. He said the vishers had routed their message through an Oakland, Calif., health insurance company's Web site.

Prindle said by using something called spam zombies to infect the legitimate Web site, vishing messages appear to be coming from a legitimate organization, thus bypassing the spam-blocking software that would ordinarily filter out such illicit messages.

"Most people have spam-blockers on now ... so the bad guys have had to think about 'How can I get my spam e-mail out?'" Prindle said.

"Well, they do it with spam zombies. ... They infect (a legitimate company's) computers with Trojans that allow their e-mails to get out to your e-mail."

The net effect of all this on the economy is hard to say, although some reports show total phishing losses are approaching \$3 billion. And the number of incidents only seems to continue to grow.

A joint U.S.-Canadian report released last October showed the number of phishing messages increased 81 percent in the first half of 2006 over the previous six months, in data collected for the Symantec Internet Security Threat Report. Prindle said the picture is no different locally, where the number of all computer-based crimes continues to soar.

"I would estimate that 75 percent of (phishing scams) come from outside the U.S., mostly from eastern Europe and northwest Africa," Prindle said.

"It's my opinion that a lot of these are used to fund terrorist activity against the U.S. ... And really it (phishing) is a terrorist activity, too, because it undermines our faith in our financial institutions."

Authorities say that regardless of whether you responded to a phishing e-mail or Web site, you should report any suspicious messages. Prindle recommends that consumers notify the Internet Crime Complaint Center by filing a complaint on the organization's Web site, www.ic3.gov.

The center is a joint venture of the FBI and the National White Collar Crime Center, where staff analyze complaints for patterns and pass the information to appropriate local, state and federal authorities for investigation.

Computer crime fighters such as Prindle, in turn, often consult the center's data to determine if any connections exist between local incidents and others reported worldwide.

However, with the Boone County Sheriff's Department's computer forensics unit the only team working such crimes full-time in Northern Kentucky, Prindle said the number of cases has far exceeded the number of investigators for a long time.

He keeps pushing for formation of a regional computer crime unit, along with more education about the issue in schools, through programs like I-SAFE, because right now, as Prindle sees it, the criminals have the numbers working in their favor.

"I think we really have to find some kind of imaginative, aggressive way to deal with this," Prindle said.

"It's already reached epidemic proportions."