

**Risk Alert
May 2010**

Phishing, Smishing, and Vishing on the Rise

Financial institutions across the country continue to report a high volume of text message and phone phishing attacks against consumers. Many of the individuals being targeted do not belong to institution whose name appears in the text message or phone call. The automated message indicates the individual's card has been de-activated and to re-activate the card, he/she must enter their 16 digit card number, security code, card expiration date, and/or PIN. In some cases there was no number attached to the call. Some members have fallen prey to the scam and provided their card information, which resulted in subsequent fraud.

Phishing, Smishing, and Vishing: What's the Difference?

E-MAIL "PHISHING"

Phishing (pronounced "fishing") is a scam to steal valuable information such as credit card and Social Security numbers, user IDs, and passwords. In phishing, also known as "brand spoofing," an official-looking e-mail is sent to potential victims pretending to be from their ISP, credit union, bank, or retail establishment. E-mails can be sent to people on selected lists or on any list, and the scammers expect some percentage of recipients will actually have an account with the real organization.

TEXT MESSAGE "SMISHING"

Smishing (SMS phISHING) is the mobile phone counterpart to phishing. Instead of being directed by e-mail to a Web site, a text message is sent to the user's cell phone or other mobile device with some ploy to click on a link. The link causes a Trojan to be installed in the cell phone or other mobile device.

LAND LINE TELEPHONE "VISHING" & VoIP (INTERNET PHONES "VISHING")

Vishing, (Voice phISHING) also called "VoIP phishing for the Internet phones," is the voice counterpart to phishing. Instead of being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's card number or other personal or financial information. The initial bait can also be a telephone call with a recording that instructs the user to phone an 800 number or another area code within or outside of the United States. In either case, because people are used to entering card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed and the entire operation can be brought up and taken down in a short time, compared to a land line telephone.

New! Mail LETTER "PHISHING"

This new scam occurs where the phisher is creating a letter and sending it through the mail to individuals to respond to the letter by calling a phone number. The phisher

outlines in the letter that the individual must respond for their own protection. This scam is used in conjunction with other channels to steal valuable personal and financial information of the individual receiving the letter.

Follow these steps to protect yourself:

- If a message is received by someone claiming to be your financial institution asking for confidential information, NEVER respond unless you initiated the request
- If you have doubts about who the message came from, call back the number of record for the financial institution or credit card company
- Be wary of any message received from an unknown sender - In many cases, the smishing message will show that it came from "5000" instead of displaying an actual phone number. This usually indicates the the SMS message was sent via email to the cell phone, and not sent from another cell phone
- Do not open unsolicited e-mails or text messages
- Do not click on any links provided in unsolicited e-mails or text messages
- Deploy “blockers” on emails, text messaging, phone numbers, both land line and VoIP. In addition, consider “extra” caution when using “text messaging”. You may want to disable the “text messaging” feature on your mobile device if you are not using it
- Don’t display your wireless phone number or e-mail address in public. This includes newsgroups, chat rooms, Web sites, or membership directories

If you become a victim of this type of fraudulent scam:

- Report it to your financial institution or credit card company immediately
- Close any compromised cards or accounts
- Review account history and look for unauthorized transactions
- Report the incident to a credit bureau
- Order a credit report and analyze for any unauthorized activity
- Report suspicious Internet sites and emails to the government and for additional protection tips visit www.ic3.gov or the Federal government’s consumer information center at www.consumer.gov/Tech.htm.

For more information regarding “smishing”, “vishing” and “phishing”, please visit these sites:

<http://www.antiphishing.org/index.html>.

<http://www.fbi.gov/page2/feb07/vishing022307.htm>

http://www.consumeraction.gov/caw_telemarketing_vishing.shtml

<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>

<http://www.onguardonline.gov/topics/phishing.aspx>