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

August 1, 2008

Summary

Phishing scams continue to affect credit unions, but the styles of phishing are shifting. Vishing, Smishing, and U.S. Mail Phishing are new ways to bait members into divulging personal and financial information. Scammers are turning to these different methods with the hope of confusing members into thinking they can only be "phished" through the use of e-mail. These methods are defined as follows:

Details:

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.

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.

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.

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.