



Vishing Scams Use Phones Instead of Fake Websites

In a new twist, identity thieves are sending spam that warns victims that their credit union/bank accounts or PayPal accounts were supposedly compromised. However, unlike typical phishing e-mails, there is no website address in these recent messages. Instead, the victim is urged to call a phone number to verify account details.

The automated voice message says: "Welcome to account verification. Please type your 16-digit card number." The goal is to get the victim to enter his or her credit card number. In these reported scams, no mention of the credit union, bank or PayPal is made.

Security experts tracking this scam and other instances of "vishing" – short for "voice phishing" – say the frauds are particularly despicable because they imitate the legitimate ways people interact with financial institutions. In fact, some vishing attacks don't begin with an e-mail. Some come as calls out of the blue, in which the caller already knows the recipient's credit card number. This increases the perception of legitimacy, leaving the caller open to request the valuable three-digit security code on the back of the card.

Vishing appears to be prospering with the help of Voice over Internet Protocol, or VoIP, the technology that enables cheap and anonymous Internet calling, as well as the ease with which caller ID boxes can be tricked into displaying erroneous information.

Follow these important guidelines to avoid becoming a victim of phishing or vishing:

- Never call a number you receive in an e-mail, even if you recognize the company or believe the sender to be legitimate. And certainly don't divulge any private information if you make a mistake and do call. If you want to call your Credit Union, use the phone number you regularly use, not the phone number you get in an e-mail.
- Never click on a link provided in an e-mail, especially if you suspect the message is fraudulent.
- If you believe the contact is legitimate, go to the company's website by typing in the site address directly or using a page you have previously bookmarked, instead of a link provided in the e-mail.
- Do not open an attachment to an unsolicited e-mail unless you have verified the source.
- Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify information.
- Use the FTC (Federal Trade Commission) website, www.onguardonline.gov, to better inform yourself. You can take interactive quizzes designed to enlighten you about identity theft, phishing, spam and online-shopping scams. Elsewhere on the site, you can find detailed guidance on how to monitor your credit history, use effective passwords and recover from identity theft.

Quorum Federal Credit Union will never request personal or account information via e-mail or ask you to access a link and submit information. Should you receive a message of this nature, please contact us immediately at (800) 874-5544 to alert us or to confirm the validity of the message.

Source: CUNA Mutual report, July 2006