Phishing Attacks Increase Nearly 600% in 2009; Prevention Starts with Members

Criminal phishing (e-mail), smishing (text messaging) and vishing (telephone) attacks increased nearly 600 percent in 2009 according to the Anti-Phishing Working Group. Unsuspecting credit union members continue to respond to fraudsters who contact them through various methods to obtain their personal or financial information. These scams are well-designed to mimic legitimate organizations (including credit unions), so it's often too late when members realize they've been swindled.

The following are examples of phishing requests mimicking credit unions:

"Your account has been temporarily suspended because of a security breach at our credit union. Please provide your information to our security department to reactivate your account."

"Your credit card was suspended. Our customer service department needs your information to reinstate your card."

"Your loan is delinquent. Payment is needed 'immediately' (over the phone)."

"You can receive a reduced interest rate on your loan. We need to confirm your information."

This type of socially-engineered breach of personal or financial information is a potentially costly and devastating crime that can impact your credit union and your members. Fortunately, losses can often be prevented through member awareness combined with sensible everyday practices.
Members should never respond directly to requests that purport to be from a credit union or any other company, no matter how urgent or persuasive the request. Instead, members should initiate the communication using the customer service number listed on their monthly statement to verify that the request is legitimate.

RISK Scenarios:
During the last month, a number of credit unions have reported phishing, smishing and vishing scams mimicking their organizations. In one case, members were advised that they would receive a reduced interest rate on their loan if they responded to the request. Working with a leading telecommunications carrier, we successfully shut down the related telephone numbers.

Loss Prevention Recommendations:

Tips to protect members:

- Don't respond to e-mails, text messages or telephone calls asking for personal identification or financial information
- E-mails and Internet pages created by scammers may look exactly like credit unions
- Learn more about phishing scam techniques at http://www.antiphishing.org/consumer_recs.html
- Take action immediately by alerting your credit union, placing fraud alerts on your credit files, and monitoring your account statements
- Report scams to the Federal Trade Commission by calling 1-877-IDTHEFT

Protect your credit union and members through awareness and action. If you are aware of a risk, call our Credit Union Protection Response Center at 800.637.2676