SANTA MONICA SCHOOL EMPLOYEES FEDERAL CREDI TUNION

INTERNET SCAM ALERT:

Your Identity for a Free Gift Card

SCENARIO/METHOD: Phishing Survey Offers Gift Cards for Information

What is Phishing?
Phishing attacks use 'spoofed' emails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security Numbers, etc. By hijacking the trusted brands of well-known financial institutions, online retailers and credit card companies, phishers are able to convince many recipients to provide personal and financial information.

"Identity Theft 911" reports a new phishing scam that uses the promise of gift cards or merchandise from major retailers to lure recipients into providing sensitive personal and financial information.

The phishing email prompts members to fill out an online "survey" that asks for the name of their financial institution, passwords, email addresses, and other personal account information. In exchange, at least one version of the scam promises a retail gift card valued up to $500. The member will never receive the free gift card. The only thing the member will get is a headache, because his/her identity will be stolen.

With millions of Americans buying gifts online during this holiday season, fraud experts are warning consumers to be wary of scams offering gift cards or merchandise in exchange for personal or financial information.

LOSS PREVENTION RECOMMENDATIONS

- Share this information with your membership via newsletters or your credit union Web site.
- Financial institutions and members *should not access* the link or attached files provided in the body of the email.
- Financial institutions and members *should not*, under any circumstances, provide any personal information to unknown sources.
- Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar.
- Members should review credit card and other account statements as soon as they receive them to determine whether there are any unauthorized transactions.
- If the statement is late by more than a couple of days, members should call the credit card company or credit union to confirm their billing address and account balances.
- Members should report suspicious activity to the FTC. Send the actual spam/phish to uce@ftc.gov.
- If the member believes they are a victim of identity theft, they should file a complaint at www.ftc.gov, and they should visit the FTC's Identity Theft Web site (www.ftc.gov/idtheft) to learn how to minimize his/her risk of damage from the identity theft.
- Victims should place a "fraud alert" on their credit bureau records.