

# Protect Yourself from "Phishing" Scams

For members who "surf the net," have e-mail accounts or visit [secny.org](http://secny.org), we would like you to be aware of a recent security scam. Phishing is a type of fraud using e-mail that appears to be from legitimate companies in an attempt to obtain your personal information.

In recent weeks, we have seen a big increase in phishing attempts on other institutions. This is due to increased security measures being used at financial institutions. Many financial institutions have reported that their customers are now receiving phishing e-mails claiming to be their bank or credit union. The e-mail states that their account has been disabled due to security reasons or other problems and asks that they provide personal information to keep their credit card, debit card or online banking account active. These e-mails contain a link to a fraudulent Web site that appears to be exactly like their financial institution's legitimate web site. When the recipient clicks on the link in the e-mail, he or she is redirected to a fraudulent web site asking him or her to enter sensitive account information such as a name, account number, credit or debit card numbers and other personal information to keep his or her account active.

Fake Cashiers checks from purchases and sales of items over the internet. If the purchasing party sends you too much money in a form of a check and ask you to send them back the difference... it's a scam. The check bounces and you are out the money you sent. Foreign lotteries stating you have won, just send them the taxes... it's a scam. Someone needs help handling money between countries and will pay you an amount from the proceeds... it's a scam.

If you receive any e-mail message asking for your account information, **DON'T DO IT!**

As a reminder, SECNY Federal Credit Union will never send you an e-mail or call you requesting personal or confidential information. If you receive an e-mail requesting this information, please notify the credit union immediately by calling our Main Office at (315) 469-5599.

Review the following tips on how to protect your personal information:

Be suspicious of any e-mail asking for personal information or containing a link to a Web site requesting that you enter your personal information such as your name, account number, password, PIN or Social Security Number. Most legitimate companies will not ask you for this information via an e-mail. SECNY FCU will never send you an e-mail containing a link to a Web page where you are required to "Sign On" to SECNY online.

Never reply to a suspicious or unexpected e-mail informing you that your account will be closed, shut down or made inaccessible unless you confirm your account information. Do not click on any links in the e-mail.

If you are uncertain about the request, contact the company that sent the e-mail through an address or telephone number you know to be genuine.

Never provide financial information to anyone via e-mail, as it is not secure.

Forward suspicious e-mails to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov), and file phishing complaints with the State Attorney General's office or through the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov).

If you suspect that you unknowingly supplied personal or financial information on your account(s) by responding to an e-mail or on a fraudulent Web site, contact Member Services at (315) 469-5599 immediately!

SECNY FCU is working diligently to keep your account and your personal information safe.

## *Scam Alert! (May 2011)*

Recently, a few of our members have encountered "Secret Shopper" scammers sending checks in the mail to supposedly "compensate" them for participating in Secret Shopper activities for companies like Wal-Mart and other major retailers. In some cases, the scammers ask for the member to send back a certain amount of money to cover "processing fees" or other such costs. These checks turn out to be fake and the member is out the money he or she sent and also is now responsible for any returned item fees which can lead to negative balances and more trouble. The bottom line: if you receive checks from an unknown source or from a program you were unaware you signed up for, they are most likely fakes.

Another scam going around involves the scammer contacting a relative pretending to be a grandchild or child in trouble and asking the person to send money to help him or her out of the situation. The scammer typically asks if the victim knows who it is on the phone and in doing so the victim will usually reply with a child or grandchild's name, therefore supplying the scammer with the ability to impersonate that child or grandchild and get away with the money sent.