



Don't Fall Hook, Line, and Sinker for a Phishing Scam...

Internet fraudsters and scammers are constantly devising new ways to steal your money. They do this by tricking unsuspecting people into giving up their personal information that can be used to access their account and make unauthorized charges. One of the most popular ways to perform this scam, known as phishing, is to send an e-mail that appears to be from a legitimate company with which you do business. The e-mail will tell you that there has been fraud on your account, or that the company is not able to verify the information they have on file for you. The crooks will then ask you to click on a link in the e-mail and go to a website to update your information. The website that you are directed to may look legitimate, complete with the company name and logo, but the site is really a "spoof". The information that you enter is not sent to the company for verification; the information is sent to the scammer, to be used to gain access to your account and steal your money.

Phishing e-mails are deceptive because they look like they are from legitimate companies, but they all contain content that reveals they are fake. To make sure that you do not fall victim to this very common scam, here are some indicators of phishing e-mails:

Generic Greetings

The companies you do business with have your name and they will call you by your name when sending you an important e-mail or letter. Companies that do not know you and are sending a letter to the general public may use generic greetings, such as "Dear Valued Customer".

A False Sense of Urgency

Most phishing e-mails trick you into giving up your personal information with false threats, such as closing your account if you do not respond to their requests.

Fake Links

Phishing e-mails include links to websites that look like those of legitimate companies but are really "spoof" sites. The information provided on these sites is sent to the scammer and not to the company for verification. Always check the true destination of a link before you click on it. Typing a known web address into the address box instead of clicking on a link is a good idea.

Links can contain the number "1" instead of the lowercase letter "l" which can direct you to a different site all together.

Phishers use tricks like this in their links to lure people to fraudulent websites.

Misspellings and Bad Grammar

Phishing e-mails usually contain misspellings, bad grammar, missing words, and gaps in logic. Spotting these mistakes can help you to identify a phishing e-mail and avoid falling victim to this scam.

Phishing e-mails rely on uninformed people who are tricked into giving personal information to criminals. If

you receive an e-mail that asks for personal information, do not reply, and do not click on any links or attachments in the e-mail; legitimate companies do not ask for this information via e-mail. Be sure to review your statements and report any unauthorized transactions as soon as you notice them. Following these guidelines will help to protect you from the hooks that phishers are casting.



File Your Taxes with TurboTax®

With April 15th not far away, let Securityplus FCU and TurboTax® Online make filing your taxes a whole lot easier this year. Log onto www.securityplusfcu.org to file your taxes electronically. TurboTax® is updated with the new tax law changes to help you get every deduction and tax savings you deserve. It's an easy, accurate and secure way to prepare and file tax returns. Plus, it guides you through your return step-by-step, double-checks your return for accuracy and then files your return electronically.

Have your tax refund directly deposited into your Share or Checking account and receive your refund in as little as 7-12 days. Get your refund fast with TurboTax® Online, another value-added service provided by Securityplus FCU.



Loan Review Committee Replaces Credit Committee

Starting January 1, 2006, a Loan Review Committee will replace the current Securityplus FCU Credit Committee. The Loan Review Committee will handle the appeals of members whose loan applications have been denied. Members may contest the loan decision by appeal to the Loan Review Committee.

We would like to thank the Credit Committee for all their hard work. You will even see some of the same Credit Committee members on the new Loan Review Committee. The members of the new Loan Review Committee are:

- Noma K. Carter
- Kalman V. Illyefalvi
- Richard Williams, VP of Lending & Collections

We assure you that our loan officers will do everything possible to assist our members in obtaining credit for their borrowing needs. If you have questions concerning the new Loan Review Committee, please write to:

Loan Review Committee
Attn: VP of Lending & Collections
Securityplus FCU
P.O. Box 7560
Baltimore, MD 21207.