

Member Information: Protect Yourself Online

How Not to Get Hooked by a “Phishing” Scam

Phishing is a high-tech internet scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, credit union account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization that you deal with – for example, your credit union, online payment service, or even a government agency. The message usually says that you need to “update” or “validate” your account information. It might threaten dire consequence if you don’t respond. The message directs you to a website that looks just like a legitimate organization’s site, but it isn’t. The purpose of the bogus site is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

Here are some tips to protect yourself:

Do not reply to email or pop-up messages that ask for personal or financial information.

Don’t email personal or financial information. If you initiate a transaction and want to provide your personal or financial information through an organization’s website, look for indicators that the site is secure.

Review your credit union account and credit card statements as soon as you receive them. Determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call the company to confirm your billing address and account balances are correct.

Use anti-virus software and keep it up-to-date. Also make sure that your browser is up-to-date and security patches are applied.

Always report “phishing” emails by forwarding the email to the following groups:

The anti-phishing network at: reportphishing@antiphishing.com

The Federal Trade Commission at: uce@ftc.gov

The Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov

If you believe you have disclosed sensitive information about yourself through a phishing scam you should:

Contact your credit union and credit card companies immediately and alert them to the situation.

Contact the three major credit bureaus and request a fraud alert be placed on your credit report. The credit bureaus and phone numbers are:

Equifax:	1-800-525-6285
Experian:	1-888-397-3742
Transunion:	1-800-680-7289

Report any suspicious contacts to the Federal Trade Commission through internet at www.consumer.gov/idtheft or call 1-877-IDTHEFT.

Sources: “How Not to Get Hooked by a ‘Phishing’ Scam.” Walker-Clay, Inc.; “Phishing Scams: Steps You Can Take to Avoid Being the Next Victim.” Tower Financial

Protect Yourself from Identity Theft

Identity theft is a rapidly growing threat to your financial security. Nationwide, the number of reported cases is increasing at an alarming rate. A criminal who successfully steals your identity can wreak havoc on your finances and your good credit.

Follow these basic steps to avoid becoming a victim:

Don’t give out your personal information. Never reveal your account numbers, personal account information or social security numbers over the telephone, via mail or over the internet, unless you initiated the contact or know who you are dealing with.

Dispose of sensitive personal information safely. Carelessly discarded financial documents can be a treasure trove of information to a thief. Tear up or shred credit card and ATM receipts, account statements and unused credit card offers before throwing them away.

Protect your PIN numbers and other passwords. Keeping your passwords and PINs secure is essential to your financial security. Don't set up your passwords or PINs using information that can be easily obtained. *(Don't use your mother's maiden name, your birth date, the last four digits of your social security number or you phone number.)*

Only carry identifying information that you routinely use. Keep your driver's license, credit card and related items close at hand. Do not carry more identification in your wallet or purse than you need on a daily basis. Do not carry your Social Security card in your wallet unless you need it that day.

Watch your account information and billing statements. Know your billing cycles and review your monthly account statements carefully. Make sure that all charges, drafts or withdrawals are authorized.

Prevent the theft of your mail. Don't allow incoming mail to accumulate in your mailbox. Retrieve it promptly. Deposit all of your outgoing mail at post office collection boxes. Don't leave outgoing mail in your unsecured mailbox.

Review copies of your credit report. Thanks to the Fair and Accurate Credit Transactions Act, one free copy of your credit report is now available annually from each of the three major credit bureaus. We encourage you to take advantage of this opportunity to review your credit report each year. You should check it carefully for any errors and for signs of fraudulent activity. The federal government required the creation of a centralized location where consumers may reliably obtain their free credit reports. To receive your free annual credit reports:

Visit www.annualcreditreport.com or Call 1-877-322-8228

If you become a victim of identity theft, take the following steps as quickly as possible to minimize the potential damage to you:

File a police report with your local law enforcement agency. You will need a report on file in order to dispute unauthorized charges.

Contact the fraud departments of each of the three major credit bureaus to report the identity theft and request that the bureaus place a fraud alert status in your file. You are also entitled by law to receive a free copy of your credit report if you are a victim of identity theft. *To report fraud to the major credit bureaus call:*

Equifax:	1-800-525-6285
Experian:	1-888-397-3742
Transunion:	1-800-680-7289

Contact the Federal Trade Commission's toll-free Identity Theft Hotline. www.consumer.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

The FTC will take a report and place your name in the nationwide "Consumer Sentinel" consumer fraud database shared by local, state and federal law enforcement agencies.

Contact your creditors, the credit union and any other financial institution you use. Inform them of your situation and close your account.

Call the Social Security Fraud Hotline at 1-800-269-0271

If your checks are used fraudulently, contact the following:

CHEXSYSTEMS:	1-800-428-9623
CERTEGY	1-800-437-5120
NATIONAL PROCESSING COMPANY:	1-800-526-5380
SCAN:	1-800-526-5380
TELECHECK:	1-800-710-9898

For additional information on what you can do if you believe you are a victim of identity theft, visit:

www.consumer.gov/idtheft