Internet Security Awareness Program

In the rapid changing technology environment, Summit Credit Union strives to provide fast and accurate service to our members while safeguarding their assets and information. We use multi-levels of security to protect member's confidential information and are vigilant in protecting it.

Your Credit Union will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential member information.

Online Banking Security

All information within our online banking uses the Secure Socket Layer (SSL) protocol to ensure that your account information transmitted is protected. You will be required to enter your User Name and a password to access your accounts. The first time you use Home Banking 24, our online banking service, you will be asked to enter your email address, and to provide answers to three challenge questions that will be used for security.

Multi-layer Security helps protect you against identity theft and other online fraud. Once you've provided answers to the challenge questions, you can enroll the computer you are using. After you enroll a computer, you will be able to sign on from that computer without answering a challenge question each session. You can enroll multiple computers; we do not recommend enrolling public computers or computers you do not use on a regularly basis. When you sign on using a computer that is not enrolled, you will be asked to validate your identity by choosing the answer to one randomly selected challenge question.

For even better protection, you may want to activate a higher level of security called 'one-time security code.' This service requires a one-time passcode be entered each time Home Banking 24 is accessed. You are able to set up your mobile device to receive the one-time passcode via text message after entering your User Name and Password.

To send personal or account information to the Credit Union, only use the secure messaging service provided behind the Home Banking 24 login.

As fraud cases are on the rise, it is also important that you take your own measures to ensure your information remains protected.

Here are some tips on how to stay safe when conducting business online.

- Never give out any personal information including User Names, Passwords, Social Security number, or Date of Birth.
- Don't respond to email, text, and phone messages that ask for personal information. Legitimate companies don't ask for information this way.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- Don't use personal information for your user names or passwords, such as birth dates or Social Security number.
- Use websites that protect your financial information with encryption when you shop or bank online. An encrypted site has "https" at the beginning of the web address. Look for a closed padlock on your browser window and verify that you are on the correct site.
- When using public wireless networks don't access your account over an unsecured wireless network or send information to any website that isn't fully encrypted.

- Use anti-virus and anti-spyware software, and a firewall on your computer.
- Avoid accessing your account on public computers. But, if you must, always log out of your session and close the browser.
- Set your computer's operating system, web browser, and security system to update automatically.

For more information: Federal Trade Commission – www.ftc.gov/idtheft

Identity Theft

What is Identity Theft?

Identity theft happens when someone steals your personal information and uses it without your permission. It is a serious crime that can wreak havoc with your finances, credit history, and reputation – and it can take time, money, and patience to resolve. If you become a victim of identity theft, please call our Member Service Call Center immediately at 336-662-6200 or 800-632-0210.

How to protect your information

- Never give out any personal information including birthdate, Social Security number or passwords.
- Report lost or stolen checks or credit cards immediately.
- Review your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. To order your report, call 1-877-322-8228 or visit www.annualcreditreport.com.
- Read your account statements. If a statement has errors, contact the business.
- Shred all documents containing personal information: account statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices.
- Don't respond to email, text, and phone messages that ask for personal info. Legitimate companies do not ask for information this way.

For more information about identity theft and other tips on how to protect your information visit:
Federal Trade Commission: http://www.ftc.gov/idtheft
Federal Deposit Insurance Corporation Consumer Alerts: www.fdic.gov/consumers/consumer/alerts
United States Department of Justice: www.usdoj.gov/criminal/fraud

Credit Reporting Agencies

Equifax
PO Box 105069
Atlanta, GA 30349-5069
www.equifax.com
To order a report: 800-685-1111
To report fraud: 800-525-6285

Experian
PO Box 2002
Allen, TX 75013-0949
www.experian.com
To order a report: 888-397-3742
To report fraud: 888-397-3742

Trans Union
PO Box 1000
Chester, PA 19022
www.transunion.com
To order a report: 800-916-8800
To report fraud: 800-680-7289

Card Fraud

Card Fraud is on the rise. You can't always prevent it from happening, but you can make it harder for criminals to get hold of your card information. For example, keep a record of your account numbers, their expiration dates, and the phone number in a secure place to report fraud for each company.

Summit Credit Union is committed to providing you with the most advanced fraud protection solutions available. To protect you, we may restrict card usage in countries identified as having a high volume of fraudulent activity and for unusual or high risk transaction types. Be sure to review our Visa Credit Cards web page for important information when traveling outside of your state of residence or country.

If you become a victim of identity theft, please call the Credit Union immediately at 336-662-6200 or 800-632-0210.

Other fraud protection practices include:

- Don't give your account number to anyone on the phone unless you've made the call to a company you know to be reputable. If you've never done business with them before, do an online search first for reviews or complaints.
- Carry your cards separately from your wallet. It can minimize your losses if someone steals your wallet or purse. And carry only the card you need for that outing.
- During a transaction, keep your eye on your card. Make sure you get it back before you leave.
- Never sign a blank receipt. Draw a line through any blank spaces above the total.
- Save your receipts to compare with your statement.
- Open your bills promptly — or check them online often — and reconcile them with the purchases you've made.
- Report any questionable charges to the card issuer.
- Notify your card issuer if your address changes or if you will be traveling.

For more information about fraud prevention and other tips on how to protect your information, visit NCUA Fraud Prevention Center: http://www.mycreditunion.gov/fraud/Pages/default.aspx

Regulation E: Electronic Fund Transfers

Regulation E is a consumer protection law designed to protect consumer accounts established primarily for personal, family or household purposes making electronic fund transfers. Excluded from coverage are non-consumer accounts, such as Trust, Corporations, Partnership, etc. The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs, or authorizes a financial institution either to credit or debit a consumer's asset account.

Regulation E gives consumers a way to notify their financial institution that an EFT has been made on their account without their permission. If you believe an unauthorized EFT has been made on your account, contact us immediately.

Non-consumer accounts are not protected by Regulation E.

A non-consumer member using online banking and/or bill pay is not protected under Regulation E. Because the member is not protected by Regulation E, precautions should be made by the member to evaluate and review the controls in place to ensure that they are correspond with the risk level that the member is willing to accept. The member should also perform a risk assessment and evaluate the controls they have in place periodically. The risk assessment should be used to determine the risk level associated with any internet activities the non-consumer member performs and any controls in place to mitigate these risks.

Unsolicited Contact

Notify us at once if you believe your password has been lost or stolen, or an unauthorized person has obtained access to your accounts without your permission. Telephoning is the best way of keeping your possible losses down.

If you believe someone has used your Password or accessed your accounts through Online Banking without your authorization, please contact us immediately by calling 336-662-6200 or 800-632-0210.

Summit Credit Union will only contact its members regarding online banking activity on an unsolicited basis for the following reasons:

- Suspected fraudulent activity on your account;
- Inactive/dormant account;
- To notify you of a change or disruption in service; or
- To confirm changes submitted on your online banking profile.

If you receive an unsolicited contact from a Summit Credit Union staff member for any reason not stated above, your identity will be confirmed through a series of security questions and you will always have the option of hanging up and calling Summit Credit Union to confirm that validity of our request. Remember, we will NEVER ask for your log in security credentials.