Security Notice

Online Safety Tips

In today's high tech world, we are able to do things more quickly and conveniently electronically whether it is to send a letter via email, pay bills or even go shopping online. With this increase in speed and convenience also comes increased risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. At Endurance Federal Credit Union, the security of member information is a priority. We are strongly committed to the safety and confidentiality of your records. One of the best ways to avoid fraud is to become an educated member and we would like to help you in this endeavor. When performing transactions on the Endurance FCU website, it is wise to make sure that the website is legitimate and your deposits are federally insured. Here are some tips specifically designed for members to consider when performing credit union transactions over the internet.

Make Sure You Are On the Endurance Federal Credit Union

Website Copycat websites deliberately use a name or web address very similar to the website they think will provide them with access to information provided by you, Criminals use fake email addresses and fake web pages to mimic the page you think you want. The intent of such websites is to trick you into giving confidential information such as account numbers and passwords allowing them access to your funds and identity information. Always verify you have typed the correct website address before opening access to your account for completing transactions, checking your balance(s), etc. and avoid clicking a link from an email address to ensure you are taken to the proper website.

Read Key Information We Post on Our Website

We post notices and warnings we receive related to Identity Theft, Fraudulent Transactions, and other potential methods criminals are using that harm consumers and businesses. Read these regularly to be aware of the most current method being used to steal your information online.

Check Insurance Status and Website Address

You can verify the website of the credit union by going to the NCUA website from the "Find a Credit Union" page. Enter the credit union name and click the "Find" button. The NCUA website response will provide the "URL" (website address) of the credit union. Don't download that file! Opening files attached to emails can be dangerous especially when they are from someone you don't know as they can allow harmful malware or viruses to be downloaded onto your computer. Make sure you have a good antivirus program on your computer that is up-to-date. Remember "Links" Usually Move You to a Website That Is Not the Credit Union's Website and the Credit Union Is Not Responsible for Transactions Completed on Other Websites. The credit union provides links to other services our members have shown an interest historically to allow easier access. However these are just provided for convenience and are not owned by the Endurance FCU. You should read the Internet policies posted on websites you link to from the Endurance FCU website.

Regulation E Also Provides Protection to Members

Don't forget to check your periodic statements and report any transactions not authorized and/or completed by you. Electronic. Transactions that are not yours must be reported to us no later than 60 days from the statement on which the problem or error occurred. If you are business member, these protections are not available so it is recommended business members complete an internal risk analysis to ensure proper controls are in place for completing online transactions.

Keep Transactions Secure

Do not share confidential information you use to complete online access and/or transactions. The Internet is a public network so it is vital for your protection to safeguard your credit union account information, account number, credit and/or debit card numbers, Social Security or EIN/Tax Identification numbers, and confidential/personal information or data. If any or all of this type of information is breached your risks of losses increase proportionately. Contact Endurance Federal Credit Union Account Services at 800-368-2618 if you need more information.

Assess your Risk

- We recommend periodically assessing your online banking risk and put into place increased security controls where weaknesses are found; particularly for members with business accounts. Some items to consider when assessing your online banking risk are:
- Who has access to your online business accounts?
- How and where are user names and passwords stored?
- How strong are your passwords and how often are they changed? Are they changed before or after terminating an employee who had access to them?
- Do you have dual controls or other checks and balances with respect to access to online-banking transactions

Additional Cyberspace Safety Tips

If you receive an e-mail that appears to be from Endurance Federal Credit Union asking you to confirm your account, e-mail, personal information or any other such action, do not give away any Information. Endurance Federal Credit Union does not solicit personal and private member information via e-mail. If you receive suspicious e-mails from entities claiming to be Endurance FCU, please do not reply to them. In compliance with the U.S.A. Patriot Act, we are required to obtain and verify identification provided for all new account owners, using methods permitted by law.

What to Expect From Endurance Federal Credit Union

- Endurance FCU will NEVER call, email or otherwise contact you and ask for your user name, password or other online banking credentials.
- Endurance will NEVER contact you and ask for your credit or debit card number, PIN or 3 digit security code.

Rights and Responsibilities

With respect to online banking and electronic fund transfers, the Federal government has put in place rights responsibilities for both you and the credit union. These rights and responsibilities are described in the Account Information Disclosures you received when you opened your account with Endurance Federal Credit Union. You can also find them online under the notices link at: www.endurancefcu.org . Ultimately, if you notice suspicious account activity or experience security-related events, please contact the Credit Union immediately at 1-800-368-2618.

What are Phishing Scams

Phishing is a recent trend that puts your online security at risk. It involves email messages that appear to come from you financial institution, but actually originate from an imposter third party. These emails normally include a link to a Web site that asks for personal information, such as your PIN number or Social Security number. There are currently a number of scams affecting credit union members that appear to be from organizations such as the NCUA or the Credit Union National Association (CUNA). Please be cautious of emails from these organizations, especially if the request personal information. How to recognize a phishing scam:

1. Urgent language Wording that asks you to act quickly in order to protect your account

2. Request for personal account information

    - Account numbers
    - Credit card number
    - Social Security number
    - PIN numbers or other passwords
    - Mother's maiden name
    - Date of birth

3. Non-secure Web sites; All sites that ask for personal information should be secure and display the lock symbols in the status bat the bottom of your browser page.

4. Typos and grammatical errors Phishing emails and Web sites often include misspelled words or

other grammatical errors.

Report a phishing scam. If you believe you have received a fraudulent email from Endurance FCU, please contact us. Do not open any attachments or links included in the email. If you have submitted your personal information to a fraudulent email or Web site, contact Endurance FCU at 800-368-2618 or 580-255-3550 as well as any other financial institutions which you hold an account. To learn more about phishing, visit the Federal Trade Commission site.

Tips to Avoid ID theft

Keep the following tips in mind to make sure that you don't become a victim:

- Check your credit report at least twice a year.
- Shred all personal documents with a crosscut shredder before you throw them out.
- Don't leave incoming mail in your mailbox overnight.
- Deposit outgoing mail that contains any personal information at the post office or other safe, closed location.
- When selecting your PIN, don't use information such as your birthday, social security number, phone number or address.
- Make a copy of everything in your wallet, front and back, and keep it in a secure location.
- Don't leave personal information in your vehicle.
- Always take your ATM or store receipts with you.
- Never give personal information over the phone to people you are not familiar with.
- Never open email attachments from people you do not know.
- Never share personal information over email, even if you believe it's been requested by a legitimate company.

Protect Your Private Info

Protect your private information from Internet and e-mail scams. At ENDURANCE FEDERAL CREDIT UNON, your privacy is very important to us. That's why we want to let you know about e-mail scams on the Internet called "phishing", pronounced "fishing", a technique hackers use to lure online consumers to fake corporate Web sites through links sent to consumers by e-mail. The message in the e-mail often warns consumers that their account will be closed if their information is not updated or verified or that something has happened and it is necessary that account information be verified. The links within the e-mail are often pointed to Web forms that ask for bank account information such as routing numbers, account numbers, PIN numbers, passwords and Social Security numbers. It is an ENDURANCE FEDERAL CREDIT UNION policy to not send or request confidential account information through e-mail because it is not a secure form of communication. You should never enter private, personal information in a form

that was sent to you by e-mail. Here are a few ways you can protect yourself from internet and e-mail fraud (phishing):

- Never click on links in an unexpected e-mail that request confidential information. If updates to information are needed, always type in the address to the Web site in the browser.

- Before submitting confidential information through forms, make sure that you are using a secure internet connection.

- There are two ways of determining if your connection to a website is secure. First, look at the address bar at the top of your browser. If the website address begins with "https://", then you have established a secure connection to the website, but if it begins with "http://", then the connection is unsecured. Second, look for a "lock" icon in your browser's status bar in the bottom right hand corner. The lock verifies that your connection to the website is secure.

- Make sure that you have installed and run updated anti-virus and anti-spyware software. Both viruses and spyware can leave your computer vulnerable to attack and intrusion. Anti-virus and anti-spyware software will keep your computer safe from malicious software that might have installed itself or tries to install itself onto your computer. Anti-virus & anti-spyware software is especially important if you are using a broadband internet connection like DSL, cable or satellite.

- Install a Firewall, either software or hardware. A firewall will prevent attacks on your computer from the internet by determining if a requested connection is malicious or not. A firewall is especially important if you are using a broadband internet connection like DSL, cable or satellite.
- Keep your internet browser, anti-virus, anti-spyware and firewall up to date by visiting the manufacturer's website and check for software and security upgrades.
- Check and monitor your checking account, debit card, credit card statements and your credit report regularly to be sure all transactions are legitimate.
- Watch for misspelling or grammatical errors on forms requesting confidential information. Hackers often make errors while rushing to get bogus Web sites in place. If something doesn't look right, there is a good chance that it's not. ENDURANCE FEDERAL CREDIT UNION will never request a customer's personal, confidential information (bank card number, account number, social security number, personal identification number or password) through e-mail. If you should ever receive an e-mail requesting your personal, confidential information that appears to be from Endurance Federal Credit Union, do not respond to the e-mail and contact us immediately us by telephone at 800-368¬-2618 or 580-255-3550.

What to do if you become a victim. If you have become a victim of identity theft, follow the steps below:

- Report the theft to the three major credit reporting agencies: Experian, Equifax and Trans Union Corporation. (a) Request that they place a fraud alert and a victim's statement in your file. This will alert creditors to contact you before opening any new accounts or making any changes. (b) Request a free copy of your credit report to check whether any accounts were opened without your consent. (c) Request that the agencies remove inquiries and/or fraudulent accounts stemming from theft.
- Notify Endurance FCU and your other financial institutions and ask them to flag your account and contact you regarding any unusual activity. (a) If checks were stolen, place stop payments

on them. (b) If bank accounts were set up without your consent, close them. (c) If your ATM card was stolen, get a new card, account number and PIN. (d) Use Identity Theft Affidavit to dispute new unauthorized accounts.

- Notify the issuers of the credit cards you carry. If unauthorized charges appear on your legitimate credit cards or if unauthorized cards have been issued in your name. (a) Request replacement cards with new account numbers. (b) Monitor credit card bills for new fraudulent activity. (c) If found, report it immediately to the credit card issuers and credit reporting agencies.
- Check with any online accounts, merchants or payment services that you use for any fraudulent activity against your account.

- Contact your local police department to file a criminal report.

- Contact the Social Security Administration's Fraud Hotline to report the unauthorized use of your personal identification information.
- Notify the Department of Motor Vehicles of your identity theft. Check to see whether an unauthorized license number has been issued in your name.

- File a complaint with the Federal Trade Commission. Ask for a free copy of ID Theft: When Bad Things Happen in Your Good Name, a guide that will help you guard against and recover from your theft.

- Document the names and phone numbers of everyone you speak to regarding the incident. Follow-up your phone calls with letters. Keep copies of all correspondence.

Contact Information for Reporting

Internet Fraud Complaint Center

Federal Trade Commission – (877) ID Theft (438-4388)

Social Security Fraud Hotline – (800)269-0271

Equifax - www.equifax.com
Order a Report: 800-685-111
Report Fraud: 888-766-0008

Experian - www.experian.com
888-Experian 397-3742

TransUnion - www.transunion.com
800-916-8800