General On-Line Member Security & Awareness

6/6/2012

Security is Everyone's Responsibility

At Centra Credit Union we take the safeguarding of our members' personal information seriously. We believe it is every employee's responsibility to keep every member's information safe and secure. We also encourage each member to take steps in protecting their personal information. Click below for member security awareness training information

On-Line Security & Awareness Training Materials (opens website)

Security Controls and Internet Banking

Centra Credit Union employs a number of controls to assist in offering financial services in a secure manner via the Internet. These controls allow Centra to properly authenticate your identity when you access these services and protect your information as it travels over the Internet between Centra and your access device (such as a PC or wireless device).

Centra Credit Union's Internet Banking service requires the use of secure browsers to protect you while you access our online services. Secure browsers allow you to communicate with these services in a protected session by encrypting the information. Centra Credit Union has also implemented an Extended Validation Certificate from VeriSign to provide an added assurance that our website is not only secure, but authentic. Members should look for the green bar to ensure they are on the credit union's Internet Banking system. Other security controls implemented by Centra Credit Union include firewalls, antivirus and anti-spam software, database encryption and multifactor authentication. Additional safeguards include a timeout feature to automatically log users out of the system based on an inactivity period.

Electronic Banking Member Awareness

Centra Credit Union understands that your trust in us depends on how well we keep your personal, business, and account information secure. Centra Credit Union has a comprehensive Information Security Program to ensure your information is secure whether you choose to bank with us through credit union offices, ATMs, telephone, or the Internet.

Centra Credit Union utilizes industry-accepted security practices that are appropriate for the way you choose to bank with us. For your protection, no matter which channel you choose, we will verify your identity before granting you access to your accounts.

Centra Credit Union will never send unsolicited emails asking you to provide, update or verify personal account information such as passwords, Social Security Numbers, PINs, credit or debit card numbers, or other confidential information.

The following are some steps you can take to keep your money secure:

Password Precautions

- Password-protect your computers and mobile devices. Use automatic screen locks.
- Never disclose your PIN or password or any other security information.
- Store your mobile devices in a secure location.
- Do not store passwords on your mobile device
- Do not use Social Security Numbers, birthdates, or names as a username or in passwords. Change your passwords regularly and use combinations of letters, numbers (upper and lower case), and "special characters".

- Do not use your online banking password as a password for other online accounts.
- Do not write passwords down or share them with anyone.
- If you have selected security questions on other websites, avoid using the same questions to protect your Centralink online account.

Web Precautions

- Always make it a point to clear the browsing history or cache.
- Only download programs or applications from trusted sources.
- Make sure your computer has anti-virus and anti-spam software installed and set to automatically install updates. Ensure operating systems are always updated with the latest security patches.
- Consider the use of a personal firewall to prevent hackers from gaining access.
- Ensure websites used for transactions and shopping are secure. Look for the padlock and https.
- Always log off from any website and close your browser after making a purchase.
- Avoid the use of public computers (such as a library or cyber café) for online banking activity and secure transactions.
- Don't leave your computer while you are logged into Internet Banking.
- If you are going to access your account on a public computer take the following precautions:
    1. If using Internet Explorer, before you access Centra's web site, go first to the menu bar at the top of the browser, choose "Tools" and then "Internet Options". In the dialog box that appears, click on the "Content" tab, then click on the "Auto Complete" button and uncheck all Auto Complete buttons.
    2. At the end of your session logout of Internet Banking. Then choose "Tools" and then "Internet Options". Click on the button to "Delete Temporary Files" and then click "OK".
    3. Close the browser completely.
- Be alert for suspicious ("phishing") emails.
- Be alert for suspicious ("spoofing") websites.

ATM

- Be aware of your surroundings at the ATM. Use well-lit locations.
- Have your card ready. Avoid having to go through your wallet or purse.
- Be observant for tampered or altered ATMs. If so, don't use.
- Memorize your PIN. Don't write any PIN numbers down.
- Make sure others can't see the keypad while you are entering your PIN.
- Secure your cash and card before leaving the ATM.

Credit/Debit Cards

- Do not disclose card information to anyone.
- Sign the backs of cards as soon as you receive them.
- Memorize your PIN. Don't write any PIN numbers down.
- Keep card numbers in a secure location to help facilitate the cancellation of the cards if the cards become lost or stolen.
- Notify issuers with any change of address.
- Only carry the minimum number of cards you actually need.
- Be alert for skimmer devices.
- Open bills and statements promptly. Verify charges. Sign up for transaction alerts.
- Do not let other people use your card. If your Centra card is lost or stolen, report it to Centra Credit Union immediately to reduce your possible liability.

- Treat your cell phone like an electronic purse or wallet.

Fraud & Identity Theft

Identity thieves access personal information through credit card and bank statements stolen from mailboxes, e-mail solicitations such as phishing, and by other means. Follow these suggestions to prevent or recognize the signs of possible identity theft or fraud.

Watch for signs of fraud

- You see unexpected charges on your account.
- Your credit report shows accounts that are not yours or contains inaccurate information.
- Bills or statements you still receive by US mail stop arriving. This could mean an identity thief has taken over your account and changed your billing address.
- Your banking statement shows checks are significantly out of order.
- You receive credit cards without applying for them.
- You are denied credit for no apparent reason.
- You receive notice that you have been denied credit but did not apply for credit.
- You receive calls or letters from debt collectors & businesses about merchandise you didn't buy.

What steps can be taken to reduce the risk of Identity Theft?

1. Never provide personal financial information in response to an unsolicited Internet or telephone request. Personal information includes your SSN, account numbers and passwords. **Centra or any other financial institution would never ask you to verify your account information online**.

2. Do not be intimidated by an e-mail or a caller who threatens actions based on failure to respond to their request. Thieves will often use the threat of dire consequences if you do not immediately provide or verify financial information.

3. If you believe the contact may be legitimate, contact the financial institution yourself. Call the institution directly, or go to the company's web site by typing in the site address directly or using a page you have previously book marked, **instead of a link provided in the email**. If you receive an email from Centra that you are unsure that is legitimate you can contact our Contact Center at 1-800-232-3642 to verify the email.

4. Monitor your accounts. Review account statements regularly to ensure all charges are correct. Use online tools. Utilize electronic statements and Internet Banking to review activity online. Also take advantage of any online banking alert notification capabilities. It can help you catch suspicious activity.

5. Remember that identity theft can occur any time, not just immediately after your personal information has been fraudulently obtained. So, be vigilant and monitor your account activity and credit history regularly.

Other Prevention Tips:

- Never leave your wallet, purse, checkbook or credit receipts in your car. Car prowl is a prime source for identity theft. Thieves know to look in merchandise bags for credit receipts – which often print your credit card number.

- Have your mail delivered to a secure location. Don't place bills with signed checks in unsecured mail boxes. Mail box theft is another common source for identity thieves. Your credit card bill has everything a criminal needs to make purchases by telephone or on the Internet, and signed checks can be altered and cashed or used fraudulently.

- Be careful when using a credit or debit card. Use a secure browser when sending credit card or debit card numbers over the Internet. Review your bill/statement carefully as soon as you receive it. Dispute any unauthorized charges in a timely manner.

- Keep a list of all your credit/debit cards, card numbers and issuer phone numbers. This will facilitate your reports to creditors/banks if your purse or wallet is stolen.

- Memorize the personal identification number (PIN) for your ATM or debit card. Never store the PIN in your purse or wallet.

- Shred your financial garbage, including credit receipts, pre-approved credit offers and credit checks. Cross-cut shredders are most effective.

- Never carry anything with your SSN on it. If your health insurance card shows your SSN, ask your insurer for a new card without the SSN. Until you get your new insurance card, carry it only when you need to use it.

- Prevent credit reporting agencies from selling your name, SSN, address and credit rating. Merchants who want to offer you credit cards or sell you merchandise buy your financial information. This is a source for personal information that can ultimately be published on the Internet. Contact the "Opt out" option of all credit reporting agencies. Consider signing up for credit monitoring services.

- Know the scams – Here are some typical identity theft scams:
    - You are notified by phone, email, or letter that you won a prize or lottery, but you don't remember entering it.
    - You are asked to pay money in advance for "administration fees" or "taxes" prior to receiving a prize or winnings.
    - You are promised to receive a huge sum of money in return for using your bank account to send or receive money.
    - You are promised to make extra money working at home in return for using your bank account to send or receive money.
    - You are required to pay a fee in advance to stop foreclosure, modify a loan, or receive advice from a company or individual to stop paying your mortgage.

What steps should be taken if Identity Theft is suspected?

1. Contact Centra Credit Union immediately at 1-800-232-3642 or by visiting anyone of Centra Credit Union's branches and alerting us to the situation.

2. Report all suspicious contacts to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft or by calling 1-877-IDTHEFT.

3. Contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. The credit bureaus can also provide you with a copy of your credit report.

Here is the contact information for these credit bureaus:

Equifax
P.O. Box 740250
Atlanta, GA 30374
1-800 525-6285 (Fraud)
1-800 685-1111 (Credit Reports)
www.equifax.com

Experian
P.O. Box 1017
Allen, TX 75013
1-888 397-3742 (Fraud)
1-888 397-3742 (Credit Reports)
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92634
1-800 680-7289 (Fraud)
1-800 888-4213 (Credit Reports)
www.transunion.com

4. The law requires the three major credit bureaus to provide you with a free copy of your credit report each year, if requested. Credit reports contain information about you, including the accounts you have and your bill- paying history. Visit www.annualcreditreport.com or call 1-877-322-8228 to order your free annual report. If you have questions or concerns about any of the information you see on your credit report, you can contact the appropriate credit reporting company listed above.

Other Contacts:

- Federal Trade Commission. Accepts complaints from ID theft victims: Identity Theft Hotline: 1-877-IDTHEFT(438-4338), or, Identity Theft Clearinghouse, FTC, 600 Pennsylvania Ave. NW, Washington, D.C. 20580. To request the booklet "ID Theft, When Bad Things Happen to Your Good Name:" (877) FTC-HELP (382-4357), or mail a request to the FTC, Consumer Response Center at the above address. Find more ID theft information at www.consumer.gov/idtheft.

- Social Security Administration. If you believe your SSN has been used by a stranger: (800) 269-0271, or SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD. 21235. Fax: (410) 597-0118. www.ssa.gov.

- U.S. Postal Service. If theft of U.S. Mail is involved, or if the identity thief filed a change of address with the post office, contact the U.S. Postal Inspector: www.usps.com/postalinspectors/fraud.

Your Liability for Unauthorized Electronic Transactions

Consumer Accounts

This section applies only to transactions from consumer accounts.

*Generally***.** Tell us AT ONCE if you believe your card and/or code has been lost or stolen, or if you believe that an electronic fund transfer has been made without your permission using information from your check. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your account (plus your maximum overdraft line of credit). If you tell us within 2 business days after you learn of the loss or theft of your card and/or code, you can lose no more than $50 if someone used your card and/or code without your permission.

If you do NOT tell us within 2 business days after you learn of the loss or theft of your card and/or code, and we can prove we could have stopped someone from using your card and/or code without your permission if you had told us, you could lose as much as $500.

Also, if your statement shows transfers that you did not make, including those made by card, code or other means, tell us at once. If you do not tell us within 60 days after the statement was mailed to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time.

IF YOU NOTICE ACTIVITY ON YOUR ACCOUNT THAT APPEARS SUSPICIOUS, CONTACT US: by phone at 800-232-3642 or by visiting any Centra branch location.

Business Accounts

Business accounts do not have the benefit of limited liability protection as consumer accounts do under Federal regulation. Therefore, Centra Credit Union recommends that businesses evaluate the risks of electronic banking and implement appropriate internal controls. This should at the least include:

- A list of the risks related to online transactions that your business faces including Conducting Your Transactions Online
    - Passwords being written down and left out in the open
    - The use of old or inadequate passwords
    - The possibility of internal fraud or theft
    - Delays in terminating the rights of former employees
    - The lack of dual control or other checks and balances over individual access to online transaction capabilities

- An evaluation of controls your business uses may include
    - Using password protected software to house passwords in
    - Conducting employee background checks
    - Initiating a policy and process to terminate access for former employees
    - Segregating duties among two or more people so no one person has sole access or control
    - Conducting internal or third party audits of controls
    - Using firewalls to protect from outside intrusion or hackers