Scams

Scammers sometimes pretend to be government officials to get you to send them money. They might promise lottery winnings if you pay "taxes" or other fees, or they might threaten you with arrest or a lawsuit if you don't pay a supposed debt. Regardless of their tactics, their goal is the same: to get you to send them money. Don't do it. Federal government agencies and federal employees don't ask people to send money for prizes or unpaid loans. Nor are they permitted to ask you to wire money or add money to a prepaid debit card to pay for anything. Before you get caught in this type of scam, look for indicators:

- **You've "Won" a Lottery or Sweepstakes –** Someone claiming to be a government official calls, telling you that you've won a federally supervised lottery or sweepstakes.
- **You Owe a Fake Debt –** You might get a call or an official-looking letter that has your correct name, address and Social Security number. Often, fake debt collectors say they are with a law firm or a government agency – for example, the FTC, the IRS or a sheriff's office. Then, they threaten to arrest you or take you to court if you don't pay on a debt you supposedly owe.

Five ways to beat a government imposter scam:

1. Don't wire money.
2. Don't pay for a prize.
3. Don't give the caller your financial or other personal information.
4. Don't trust a name or number.
5. Put your number on the National Do Not Call Registry. Register you number at donotcall.gov.

Phishing is when internet fraudsters impersonate a business to trick you into giving them your personal information, such as usernames, passwords, and credit card details. Legitimate businesses don't ask you to send sensitive information through insecure channels.

For example, a fraudulent e-mail may state that MCUA will add money to the member's account for taking part in a survey. The link embedded in the message directs members to a counterfeit version of the NCUA's website with an illicit survey that solicits credit card account numbers and confidential personal information. NCUA will never ask credit union members or the general public personal account or personally identifiable information as part of a survey.

Tips:

- **Don't select links in e-mails that ask for personal information.**
- **Never open unexpected attachments.**
- **Delete suspicious messages, even if you know the source.**

Smishing uses cell phone text messages to trick you into providing personal and financial information. Smishers may use URLs or an automated voice response system to try and collect your information.

Tips:

In some instances, criminals have used malicious software in their text messages solicitations. To prevent further security issues, completely remove unsolicited text messages from your phone. This may take two steps: deleting the text and then completely removing it from your device.

Vishing exploits a general trust in landline telephone services. The victim is often unaware that voice over Internet Protocol (VoIP) allows for caller ID spoofing, thus providing anonymity for the criminal caller. Rather than providing any information to the caller, the consumer should verify the call by contacting the financial institution or credit card company directly, being sure to use the institution's accurate contact information (i.e., don not use contact information the caller provides).

Online Gift Card Scam

Gift cards purchased through online auction sites are often fraudulent or stolen. To ensure that you are not scammed out of your money, it is safest to purchase gift cards directly from the merchant or retail store.

Stripped Gift Card Scam

Be careful when purchasing gift cards in retail stores. If you choose a gift card that is not located behind a counter, thieves can write down the gift card code or use a device to scan the magnetic strip on the back of the card. Every few days the thief will check the balance and redeem the card's value online without you or your gift recipient's knowledge. When buying a preloaded card, always have the cashier scan the card to verify the full amount is available. Also, check to make sure that the packaging has not been tampered with or damaged. This may be a sign that the gift card has been compromised or replaced with a stripped gift card. If possible, register your gift card with the retailer.

Charity Scams

It is important to recognize the warning signs of charity scams in order for you not to be robbed of your good intentions. The Federal Trade Commission (FTC) has two websites for consumers on charity fraud and scams.

- Before Giving to a Charity (FTC)
- Charity Scams (FTC)

In addition, the Internal Revenue Service (IRS) has a search feature on its website that allows consumers to find legitimate, qualified charities to which donations may be tax-deductible.

Fraudulent Classified Ads and Auction Sales

Internet criminals post classified ads and auctions for products they do not have and make the scam work by using stolen credit cards. Fraudsters receive and order from a victim, charge the victim's credit card for the amount of the order, then use a separate, stolen credit card for the actual purchase. They pocket the purchase price obtained from the victim's credit card and have the merchant ship the item directly to the victim. Consequently, an item purchased from an online auction but received directly from the merchant is a strong indication of fraud. Victims of such a scam not only lose the money paid to the fraudster, but may be liable for receiving stolen goods.

Shoppers may help avoid these scams by using caution and not providing financial information directly to the seller, as fraudulent sellers will use this information to purchase items for their schemes. Always use a legitimate payment service to ensure a safe, legitimate purchase.

As for product delivery, fraudsters posing as legitimate delivery service offer reduced or free shipping to customers through auction sites. They perpetuate this scam by providing fake shipping labels to the victim. The fraudsters do not pay for delivery of the packages; therefore, delivery service providers intercept the packages for nonpayment and victim loses money paid for the purchase of the product.

Diligently check each seller's rating and feedback along with their number of sales and the dates on which feedback was posted. Be wary of a seller with 100 percent positive feedback, with a low total number of feedback postings, or with all feedback posted around the same date and time.

Here are some additional tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) email.
- Do not click on links contained within an unsolicited email.
- Be cautious of email claiming to contain pictures in attached files, as files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Log directly onto the official website for the business identified in the email, instead of "linking" to it from an unsolicited email. If the email appears to be from your financial institution, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- Contact the business that supposedly sent the email to verify if the email is genuine.
- If you are asked to act quickly, or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.

Report a Scam
If you get a call from an imposter, file a complaint at ftc.gov/complaint. Be sure to include:

1. Date and time of the call,
2. Name the imposter used,
3. What they tell you, including the amount of money and the payment method they asked for, and
4. Phone number of the caller; although scammers may use technology to create a fake number or spoof a real one, law enforcement agents may be able to track that number to identify the caller.

Cyber crime includes more than fraudulent e-mail messages and fake websites that allow criminals to take your money. A cyber crime may involve tactics using ransomware, where criminals lock you out of your files until they receive a ransom, or phony phone calls, such as criminals pretending to represent a tech support company so they can get your information. Protect yourself from a range of cyber crimes by taking these precautions:

- Use a firewall to protect your computer.
- Encrypt your home Wi-Fi network.
- Back up your files regularly.
- Create strong passwords and share them only when necessary.
- Don't respond to spam e-mails.
- Monitor your financial accounts regularly for fraudulent activity.
- Download with caution.
- Don't visit suspicious websites or follow links to sources you don't trust.
- Keep your computer current by updating antivirus software, antispyware, operating system and system patches.
- Don't share your personal information with sources you don't trust, especially pop-ups.
- Have different passwords for work related and non-work related accounts.
- When you're not using your computer, turn it off.
- Don't give control of your computer to an unauthorized third party.

IDENTITY THEFT…HELP FOR VICTIMS

1. Contact the fraud departments of the 3 major credit bureaus:
   Equifax: 1-800-525-6285
   Experian: 1-888-397-3742
   TransUnion: 1-800-680-7289
2. Notify your financial institution
3. Inform your credit issuers
4. File a police report with your local law enforcement

For additional information and advice you can call the Federal Trade Commission (FTC) Identity Theft hotline toll-free at 1-877-IDTHEFT (438-4338) or visit their ID Theft Website at www.consumer.gov/idtheft

- Check your credit report annually
- Review your bills and statements on a regular basis
- Guard your mail and trash from theft
- Use caution when giving out personal information
- Copy the contents of your wallet or purse
- Report lost or stolen checks or credit cards immediately

FACTA INFO

We may furnish negative information to consumer reporting agencies. We may report information about your account to credit bureaus.

Late payments, missed payments, or other defaults on your account may be reflected in your credit report. Please make your payments on time and always pay at least the minimum amount due to assure that negative information regarding your accounts with us will not appear on your credit report.

BE A **CAUTIOUS** INTERNET USER

Internet scammers are tricking unsuspecting victims by going "Phishing". They use e-mails to lure people into fake websites to obtain personal information and commit identity theft. Victims receive fraudulent e-mails containing authentic looking logos and familiar graphics. These e-mails will lead you to a fake site, even though it looks authentic. You will be asked to divulge account information and other personal data.

We already have your personal data so we will not send you an e-mail or call you by phone asking for this information. Be suspicious if someone claiming to be from your financial institution asks for confidential information. Please review statements closely and report any suspicious activity immediately.

Change your online banking and shopping account passwords often, experts suggest every three to six months. Remember to use a combination of letters, both upper and lower case, numbers and symbols.

How you can boost **your** credit score?

1. Pay bills on time. Responsible bill payment makes up about 35% of your credit score.
2. Keep and use old cards. The older and more established your credit history, the better.
3. Ease up on "charge-its". Big balances will hurt your score. Keep balances less than 25% of your available limit.
4. Follow up on goofs. If you slipped up once and paid late, write and ask that the ding be deleted from your file.
5. Mix up your credit (mortgage, credit card or two, a personal loan and a charge card). Having a mix of credit makes up about 10% of your score.
6. Watch those new credit offers. Too many inquiries can hurt your score.
7. Check your reports for credit cards and other loans that are not yours.
8. Look for duplicate items
9. Dispute errors.
10. Credit bureaus are required to investigate mistakes that you bring to their attention.
11. Pay down your balances.
12. Lenders look at your available credit on cards and credit lines.

The higher your credit scores, the better chance you have of getting a loan or credit card application approved. You can get free copies of your credit report from the three major bureaus by using the site annualcreditreport.com.

Protection from Phishing Scammers

As your credit union, we may use e-mail to communicate with you; however, we will **never** ask you to send your Social Security number, account number, password or PIN to us by e-mail. **You can always call your credit union to verify whether an e-mail is legitimate.**

Stay clear of e-mails from businesses that alert you to consumer account problems and link you to a website for financial information verification. The site may look real but it is designed to trick you into providing your account number and personal data.

To avoid being a victim, follow these simple rules:

- Be suspicious of e-mail that asks for personal or financial information.
- Check your monthly statements to verify all transactions and notify the credit union immediately of any erroneous or suspicious transactions.
- Be cautious of any business that contacts you to notify you of "problems" with your account or to entice you with prizes.

Protection from ATM/Debit card scams

Awareness can protect you from debit and credit card fraud. Another scheme fraudsters are now using is skimming. "Skimmers" are devices that are installed over an existing card reader and designed to steal card numbers and corresponding account information stored on the card's magnetic strip. They often are camouflaged to fit gas pumps and ATMs, and they may be equipped with hidden cameras. The cameras take snapshots of debit card PIN numbers as consumers enter them. Once the scammers have acquired the account information, they use it to make a bogus card and then unauthorized purchases and withdrawals.

Follow these tips to protect your card and PIN:

- **Awareness is the best defense.** It can be difficult to avoid the scam entirely, but you can mitigate the effects by carefully monitoring your accounts.
- **Pay close attention to the card reader you are using**. If it "looks odd" or something out of the ordinary, a skimming device may be in place. Don't use it and contact the owner or manager of the company immediately.
- **Ensure that no one can see you entering your PIN**. Use your body or your opposite hand as a shield.
- **Memorize your PIN**. Never keep your card and PIN together.
- **Watch your statements and monitor your accounts online** to track debits closely. Watch for any unauthorized withdrawals or otherwise suspicious activity.
- **Try to use an ATM that is located in a very public place or is located inside a credit union or bank lobby.** Scammers are less likely to tamper with machines in those locations.

As always, contact us immediately if you suspect any fraud or notice any unauthorized transactions on your accounts.

THERE ARE MANY SCAMS GOING AROUND THAT WE ALL NEED TO PROTECT OURSELVES FROM.

One is taking your outgoing mail out of your mailbox. Thieves look for bills you are paying. They wash the check and change the name of the payee and the dollar amount. Please do not put your outgoing payments in your mailbox with the red flag up.

Another scam: People call you saying you won a prize or they need to verify your account and ask for personal information. Do not give out your debit or credit card information. Do not give out the information on the bottom of your checks.

Another scam: Someone calls saying they are a family member and they are in trouble and need you to send them money immediately. They ask you not to say anything to other family members. They tell you to wire or send them money via Western Union. DO NOT send them money. This is a scam. If you truly believe this is your family member, tell them you will call them right back on their cell phone. Do not use a phone number that they give you, only use one that you already have. Contact their immediate family and ask if the family member is really where they say they are. Unscrupulous people prey on others by upsetting them into thinking they are speaking with their family member. They use guilt tactics to get them to send money to help their "loved ones" when they are really sending money to a thief. Double and triple check all information that is given to you before you ever send money.

There are bogus emails asking for personal information or directing you to fake websites. If you do not know sent the email, do not respond.

Do not write your PIN on your ATM or Debit card.

Unless you have personally initiated the contact and with a reputable company, do not give out your information. The credit Union will never call asking for person information.

Warning Signs of Fraudulent Offers

- A promise that you can win, make, or borrow money easily.
- A demand that you act immediately or else miss out on a great opportunity.
- A refusal to send you written information before you agree to buy or donate.
- An attempt to scare you into buying something.
- An insistence that you wire money or have a courier pick up your payment.
- A refusal to stop calling after you have asked not to be called again.

Appendix A

The following is a list of recommendations you could share with your members to help them ***avoid*** becoming a victim of phishing scams.

- Be suspicious of any email with urgent requests for personal financial information unless the email is digitally signed (you can't be sure it wasn't forged or 'spoofed'). Phishers typically: (1)include upsetting or exciting (but false) statements in their emails to get people to react immediately; (2)ask for confidential information such as usernames, passwords, credit card numbers, social security numbers, account numbers, etc.; and (3)do not personalize the email message (while valid messages from your credit union should be).

- Don't use the links in an email to get to any web page if you suspect the message might not be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.

- Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone.

- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just http://.

- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites.

- Regularly log into your online accounts and don't wait for as long as a month before you check each account.

- Regularly check your financial institution, credit, and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact your financial institution(s) and card issuers.

- Ensure that your browser is up to date and security patches applied.

- Always report "phishing" or "spoofed" e-mails to the following groups:
    - forward the email to reportphishing@antiphishing.com;
    - forward the email to the Federal Trade Commission at spam@uce.gov;
    - forward the email to the "abuse" email address at the company that is being spoofed;
    - when forwarding spoofed messages, always include the entire original email with its original header information intact; and
    - notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/.

Appendix B

What To Do If You've Given Out Your Personal Financial Information

Phishing attacks are growing quite sophisticated and difficult to detect, even for the most technically savvy people. And many people are getting onto the Internet and using email or Web browsers for the first time. As a result, some people are going to continue to be fooled into giving up their personal financial information in response to a phishing email or on a phishing website. If you have been tricked this way, you should assume that you will become a victim of credit card fraud, financial institution fraud, or identity theft. Below is some advice on what to do if you are in this situation:

- Report the theft of this information to the card issuer as quickly as possible:
  - Many companies have toll-free numbers and 24-hour service to deal with such emergencies.
- Cancel your account and open a new one.
- Review your billing statements carefully after the loss:
  - If they show any unauthorized charges, it's best to send a letter to the card issuer describing each questionable charge.
- Credit Card Loss or Fraudulent Charges (FCBA):
  - Your maximum liability under federal law for unauthorized use of your credit card is $50.
  - If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use.
- ATM or Debit Card Loss or Fraudulent Transfers (EFTA):
  - Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss.
  - You risk unlimited loss if you fail to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you.
- Report the theft of this information to the bank as quickly as possible.

Some phishing attacks use viruses and/or Trojans to install programs called "key loggers" on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, usernames, passwords, Social Security Numbers, etc. In this case, you should:

- Install and/or update anti-virus and personal firewall software.
- Update all virus definitions and run a full scan.
- Confirm every connection your firewall allows.
- If your system appears to have been compromised, fix it and then change your password again, since you may well have transmitted the new one to the hacker.

- Check your other accounts! The hackers may have helped themselves to many different accounts: eBay account, PayPal, your email ISP, online bank accounts, online trading accounts, e-commerce accounts, and everything else for which you use online password.

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes. If you have given out this kind of information to a phisher, you should do the following:

- Report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation, and do the following:
    - Request that they place a fraud alert and a victim's statement in your file.
    - Request a FREE copy of your credit report to check whether any accounts were opened without your consent. You can find information about obtaining free credit reports on the Federal Trade Commission's website at: http://www.ftc.gov/bcp/conline/edcams/freereports/index.html.
    - Request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft.

- Major Credit Bureaus:
    - Equifax - www.equifax.com:
        - To order your report, call: 800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241.
        - To report fraud, call: 800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241.
        - Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.
    - Experian - www.experian.com:
        - To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2002, Allen TX 75013.
        - To report fraud, call: 888-EXPERIAN (397-3742) and write: P.O. Box 9530, Allen TX 75013 TDD: 1-800-972-0322.
    - Trans Union - www.transunion.com:
        - To order your report, call: 800-888-4213 or write: P.O. Box 1000, Chester, PA 19022.
        - To report fraud, call: 800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634 TDD: 1-877-553-7803.

- Notify your financial institution(s) and ask them to flag your account and contact you regarding any unusual activity:
    - If bank accounts were set up without your consent, close them.
    - If your ATM card was stolen, get a new card, account number, and PIN.

- 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.

- Notify the passport office to be watch out for anyone ordering a passport 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.

- File a complaint with the Internet Fraud Complaint Center (IFCC)
  - http://www.ifccfbi.gov/index.asp.
  - The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), with a mission to address fraud committed over the Internet.
  - For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation.

- 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.