Member Awareness Program

Me/CU's Commitment to Security

Each year more and more Americans have their identity stolen and the staff and management of Municipal Employees Credit Union (Me/CU) want to give you the information you need to help protect yourself against identity theft.

Me/CU cannot guarantee that your ID will never be stolen, but Me/CU will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential member information.

Fraudulent emails which request personal or confidential information may be designed to appear as though they are originated from Me/CU. If this information is requested in an email, even if it appears to be from Me/CU, please do not respond or go to any links listed on the email.

Me/CU will never contact you and ask for your debit/credit card number or your full SSN. If we need to contact you, it will always be done in a manner that protects your personal, confidential information and we will clearly identify ourselves. We will not ask you for information we already have.

Me/CU has multi-layer security to protect your confidential information and will continue to be vigilant in protecting it.

Please immediately report any suspicious emails or websites to Me/CU by forwarding the message to info@mecuokc.org if you suspect identity theft or have any questions regarding this notice, please contact us at 405-813-5500.

Online Banking Security

Me/CU is committed to protecting your personal information. Our Online Banking uses several different methods to protect your information. All information within our Online Banking uses the Secure Socket Layer (SSL) protocol for transferring data. SSL is a cryptosystem that creates a secure environment for the information being transferred between your browser and Me/CU. All information transferred through Online Banking has a 128-bit encryption which is the highest level of encryption. In addition to the security features put in place by Me/CU here are some tips on keeping your information secure.

- Never give out any personal information including User Names, Passwords, SSN, and Date of Birth.
- Create difficult passwords which include letters, numbers, & symbols when possible.
- Don't use personal information for your user names or passwords like Birth Dates & SSN.
- Avoid using public computers to access your Online Banking.
- Don't give any of your personal information to any websites that does not use encryption or other secure methods to protect it.

Mobile Devices:

- Use passcodes.
- Avoid storing sensitive information.
- Keep software up-to-date.
- Install remote wipe, if the device is lost or stolen it can be cleared off.

What is Identity Theft?

Identify theft occurs when someone uses your personal information such as:

- Name
- Address
- Date of Birth
- Social Security Number (SSN)
- Mother's Maiden Name
- Driver's License
- Credit Union, Bank or Credit Card Account Number

Thieves then use the information to repeatedly commit fraud in an attempt to duplicate your identity which may include opening new accounts, purchasing automobiles, applying for loans, credit cards, social security benefits, renting apartments and establishing services with utility and telephone companies. It can have a negative effect on your credit and create a serious financial hassle for you.

What is 'Phishing'?

phishing (FISH.ing): Phishing is the attempt to acquire sensitive information by masquerading as a trustworthy entity in an electronic

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

Tips to identifying “Phishing” emails:

- Awkward greeting - A phish may address the member with a nonsensical greeting or may not refer to the member by name.
- Urgent call to act - Different approaches include things such as "We're updating our records," "We've identified fraudulent activity on your account," or "Valuable account and personal information was lost due to a computer glitch." To encourage people to act immediately, the email usually threatens that the account could be closed or canceled.
- Source code points to a different website than the alleged sender - The link looks official, but when your mouse curser rolls over it the link’s source code points to a completely different web site. Remember that you can always type a URL into your web browser instead of clicking on a link.
- Typos & Incorrect Grammar - This is a technique used by phishers to avoid email filters. The errors are intentional.
- If you fall victim to an attack, act immediately to protect yourself. Alert Me/CU as soon as possible. Place fraud alerts on your credit files. Monitor your credit files and monthly statements very closely.
- Report suspicious emails or calls to the Federal Trade Commission through the Internet, or by calling 1-877-ID-THEFT.

What is 'Spoofing'?

Pretending to be something it is not, whether an email, website, etc…

Email spoofing is the creation of email messages with a forged sender address. Spoofing can be easy to do so due to the core protocols do not have any mechanism for authentication. Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message.

Insure that the site you are looking at is what it appears to be? Is it coming from the company it claims to? If the site is not an SSL secured site, perhaps because it doesn't actually use financial information but collects or uses some other personal information, you should consider carefully whether or not you want to provide any of the requested information. These sites can also be spoofed, but you won't have the SSL certificate to help you identify the spoof. Instead, this JavaScript code, copied and pasted into the address bar, will provide you with the site and server identification:
javascript:alert("The actual URL is:\t\t" + location.protocol + "//" + location.hostname + "/" + "\nThe address URL is:\t\t" + location.href + "\n" + "\nIf the server names do not match, this may be a spoof.");

What is 'Pharming'?

Fraud by directing internet users to bogus websites that appear real and then stealing information.

What is “Vishing”?

Fraud using telephones to scam users into giving up their private information. Pretends to be legitimate business and fools people into think there’s a profit to be made.

What is “Smishing”?

A security attack where a Trojan horse is downloaded, or virus or malware, on a cellphone or other mobile device.

Debit Card Protection

Debit card usage has increased dramatically in recent years and fraudulent use of debit cards has also increased. We at Me/CU have some suggestions for you for the care and usage of debit cards.

- NEVER give your debit card information when requested by phone, email, or texting.
- Me/CU will never request information from you in this manner. Please contact us if you receive any such request.
- It is a good idea to pay by credit card if your card leaves your sight.
  An example might be when a waiter takes your card from your table in a restaurant or when ordering online. Debit cards are easier to process illegally than credit cards.
- Install and keep up to date antivirus software protection.
- Be sure and use a firewall when surfing.
- Don't click on links in emails.
- Don't surf to pages you are unsure of.
- If you have a business account you should perform your own risk assessments and evaluations on all online accounts.

Using ATM’s safely:

- Protect your ATM card and PIN. If lost report as soon as possible.
- Choose a PIN different from your address, telephone #, and date of birth.
- Be aware of people and your surroundings.
- Put away your card and cash.
- Skimming - observe the card reader; if it appears damaged don't use it.
- Never give your debit card information when requested by phone, email, or texting.

How do I protect myself?

- Report lost or stolen checks or credit cards immediately.
- Never give out any personal information including date of birth, SSN or Passwords.
- Shred all documents containing personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings and invoices.
- Don't give any of your personal information to any websites that do not use encryption or other secure methods to protect it.

For more information about identity theft and other tips on how to protect yourself and your information please visit the following websites.

Caution-By clicking on the links below you will be leaving Me/CU's secure website.

Computer Security:
www.onguardonline.gov
Federal Trade Commission:
www.ftc.gov/bcp/edu/microsites/idtheft
FDIC Consumer Alerts:
www.fdic.gov/consumers/consumer/alerts
United States Department of Justice:
www.usdoj.gov/criminal/fraud
NACHA Fraud Resources:
https://www.nacha.org/Fraud-Phishing-Resources
US Department of Homeland Security:
http://www.us-cert.gov/home-and-business/
Federal Communication Commission - Business Cyber-planner:
http://www.fcc.gov/cyberplanner
Protecting Personal Information: A Guide for Business
https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure
Business Peer to Peer File Sharing:
https://www.consumer.ftc.gov/articles/0016-p2p-file-sharing-risks
Protecting the Consumer:
https://www.ftc.gov
Consumer Action: Complaints
https://www.usa.gov/consumer-complaints
FDIC Consumer Protection
http://www.fdic.gov/consumers/
Verify Personal Credit Information
https://www.annualcreditreport.com

Check Your Credit

Any consumer can request one free copy of his or her credit report per year. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name. Contact the three major credit bureaus:

- 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

Regulation E: Electronic Fund Transfers

How Does Regulation E Apply to Your Accounts with Internet Access?

Regulation E protects individual consumers engaging in electronic fund transfers (EFT). Non-consumer or business accounts are not protected by Regulation E.

What is an EFT?

The electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions initiated through electronic-based systems. The term includes, but is not limited to:

- Point-of-sale transfers
- Automated Teller Machine (ATM) transfers
- Direct deposits or withdrawal of funds
- Transfers initiated by telephone
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal
- Transfers initiated through internet banking/bill pay

How does Regulation E apply to a consumer using internet banking and/or bill pay?

Regulation E is a consumer protection law for accounts established primarily for personal, family, or household purposes. Non-consumer accounts, such as Corporations, Partnerships, Trusts, etc. are excluded from coverage. Regulation E gives consumers a way to notify their financial institution that an EFT has been made on their account without their permission.

Important Information for Business/Commercial Members

Business/Commercial members are not covered by Regulation E. As a result, it is critical that Business/Commercial members implement sound security practices within their places of business as outlined in this Program to reduce the risk of fraud and unauthorized transactions from occurring.

Corporate Account Takeover is a form of identity theft in which criminals steal your valid online banking credentials. The attacks are usually stealthy and quiet. Malware introduced onto your systems may go undetected for weeks or months. Account-draining transfers using stolen credentials may happen at any time and may go unnoticed depending on the frequency of your account monitoring efforts.

The good news is, if you follow sound business practices, you can protect your company:

- Use layered system security measures: Create layers of firewalls, anti-malware software and encryption. One layer of security might not be enough. Install robust anti-malware programs on every workstation and laptop. Keep the programs updated.

- Manage the security of online banking with a single, dedicated computer used exclusively for online banking and cash management. This computer should not be connected to your business network, should not retrieve any e-mail messages, and should not be used for any online purpose except banking.

- Educate your employees about cybercrimes. Make sure your employees understand that just one infected computer can lead to an account takeover. Make them very conscious of the risk, and teach them to ask the question: “Does this e-mail or phone call make sense?” before they open attachments or provide information.

- Block access to unnecessary or high-risk websites. Prevent access to any website that features adult entertainment, online gaming, social networking and personal e-mail. Such sites could inject malware into your network.

- Establish separate user accounts for every employee accessing financial information, and limit administrative rights. Many malware programs require administrative rights to the workstation and network in order to steal credentials. If your user permissions for online banking include administrative rights, don’t use those credentials for day-to-day processing.

- Use approval tools in cash management to create dual control on payments. Requiring two people to issue a payment – one to set up the transaction and a second to approve the transaction – doubles the chances of stopping a criminal from draining your account.

- Review or reconcile accounts online daily. The sooner you find suspicious transactions, the sooner the theft can be investigated.

Unsolicited Member Contact

Me/CU will never contact its members on an unsolicited basis to request their security logon credentials such as the combination of the member’s username and password. If you receive a request of this type, do not respond to it. Please call us immediately at 405-813-5500 or e-mail us at info@mecuokc.org to report any activity of this nature.

Me/CU 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 to your online banking profile.

If you receive an unsolicited contact from a Me/CU staff member for any reason not cited above, your identity will be confirmed through a series of security questions and you will always have the option of hanging up and calling Me/CU to confirm that validity of our request. Remember, Me/CU will NEVER ask for your logon security credentials.

Business/Commercial

Self-Assessment

Online Banking Business/Commercial members are strongly encouraged to perform an annual Self-Assessment focusing on their online banking practices and network security. A Self-Assessment will evaluate whether the client has implemented sound business practices to address the five key principles outlined in the “Securing Your Business” section.

Securing Your Business

Is your company keeping information secure?

Are you taking steps to protect sensitive information? Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

- Take stock. Know the nature and scope of the sensitive information contained in your files and on your computers.
- Scale down. Keep only what you need for your business.
- Lock it. Protect the information in your care.
- Pitch it. Properly dispose of what you no longer need.
- Plan ahead. Create a plan to respond to security incidents.

The following information is provided by the Federal Trade Commission, Bureau of Consumer Protection.

Take Stock

Know the nature and scope of the sensitive information contained in your files and on your computers.

- Take inventory of all file storage and electronic equipment. Where does your company store sensitive data?
- Talk with your employees and outside service providers to determine who sends sensitive information to your business, and how it is sent.
- Consider all of the methods with which you collect sensitive information from customers, and what kind of information you collect.
- Review where you keep the information you collect, and who has access to it.

Scale Down

Keep only what you need for your business.

- Use Social Security Numbers only for required and lawful purposes. Don’t use SSNs as employee identifiers or customer locators.
- Keep customer credit card information only if you have a business need for it.
- Review the forms you use to gather data — like credit applications and fill-in-the-blank web screens for potential customers — and revise them to eliminate requests for information you don’t need.
- Change the default settings on your software that reads customers’ credit cards. Don’t keep information you don’t need.
- Truncate the account information on any electronically printed credit and debit card receipts that you give your customers. You may include no more than the last five digits of the card number, and you must delete the card’s expiration date.
- Develop a written records retention policy, especially if you must keep information for business reasons or to comply with the law.

Lock It

Protect the information that you keep.

- Put documents and other materials containing sensitive information in a locked room or file cabinet.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building.
- Encrypt sensitive information if you must send it over public networks.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers.

- Require employees to use strong passwords.
- Caution employees against transmitting personal information via e-mail.
- Create security policies for laptops used both within your office, and while traveling.
- Use a firewall to protect your computers and your network.
- Set “access controls” to allow only trusted employees with a legitimate business need to access the network.
- Monitor incoming Internet traffic for signs of security breaches.
- Check references and do background checks before hiring employees who will have access to sensitive data.
- Create procedures to ensure workers who leave your organization, no longer have access to sensitive information.
- Educate employees about how to avoid Phishing and phone pretexting scams.

Pitch It

Properly dispose of what you no longer need.

- Create and implement information disposal practices.
- Dispose of paper records by shredding, burning, or pulverizing.
- Defeat “dumpster divers” by encouraging your staff to separate the information that is safe to trash from sensitive data that needs to be discarded with care.
- Make shredders available throughout the workplace, including next to the photocopier.
- Use a “wipe” utility program when disposing of old computers and portable storage devices.
- Give business travelers and employees who work from home a list of procedures for disposing of sensitive documents, old computers, and portable devices.

Plan Ahead

Create a plan for responding to security incidents.

- Create a plan to respond to security incidents, and designate a response team led by a senior staff person(s).
- Draft contingency plans for how your business will respond to different kinds of security incidents. Some threats may come out of left field; others — a lost laptop or a hack attack, to name just two — are unfortunate, but foreseeable.
- Investigate security incidents immediately.
- Create a list of who to notify — inside or outside your organization — in the event of a security breach.
- Immediately disconnect a compromised computer from the Internet.

Me/CU Contacts

You are protected in a variety of ways when you use Internet Banking; however it is important to contact Me/CU in the event your company’s online access has been compromised. Also, report any unauthorized or unexpected transactions immediately.

Your account is protected against fraudulent transactions in a number of ways, so monitor your account balances and transactions frequently. If you want to report suspicious activity in your account(s), or if you have questions about the security of your account(s), you can call us at: 405-813-5500 or e-mail us at info@mecuokc.org.

Additional Resources

The following links are provided solely as a convenience to our Business/Commercial Online Banking clients. Me/CU neither endorses nor guarantees in any way the organizations, services, or advice associated with these links. Me/CU is not responsible for the accuracy of the content found on these sites.

Caution-By clicking on the links below you will be leaving Me/CU’s secure website.

Identity Theft, Privacy, and Security Publications for Businesses
http://www.business.ftc.gov/privacy-and-security
OnGuard Online - Learn how to avoid Internet fraud, secure your computer, and protect your personal information.
http://www.onguardonline.gov/
National Institute of Standards and Technology (NIST)'s – Computer Security Resource Center
http://www.nist.gov/
SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Controls
http://www.sans.org/critical-security-controls/
U.S. Computer Emergency Readiness Team
http://www.us-cert.gov/
Carnegie Mellon Software Engineering Institute's CERT Coordination Center

http://www.cert.org/