Return to eecu.org

Identity Theft

At EECU, protecting our Members from Identity Theft is a major concern. The following information has been assembled in order to educate Members about this very important matter.

What is Identity Theft?

Identity Theft is one of the fasting growing crimes in America today. Often, the victim won't even know his/her identity has been stolen until hundreds or even thousands of dollars have been spent in their name. Identity Theft is the use of someone's identity in order to impersonate them. This can include:

- Opening a new credit card account using your name, date of birth, and Social Security number
- Establishing cell phone or Internet service in your name
- Opening a new bank account, obtaining a credit card, or taking out a loan in your name
- Writing counterfeit checks or making electronic fund transfers from your account
- Changing the mailing address on your credit card account or completing a "change of address form" to divert all mail to another location.

Keys to Your Identity

The following are keys to your identity:

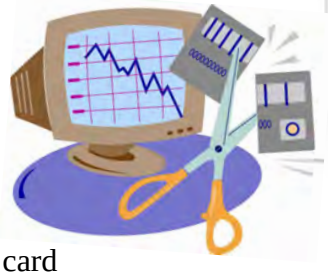
- Name
- Address
- Date of birth
- Social Security number
- Driver's license number
- Account numbers
- Passwords for online accounts
- Mother's maiden name
- PINs for debit cards or audio response systems
- Code word (an EECU specific item)

How Does Identity Theft Happen?

Identity Theft can start in a number of ways. The following are the main categories:

- Wallet or purse theft – Wallets or purses left unattended (e.g. - in shopping carts or on the seat of a car while getting gasoline) are especially vulnerable.
- Finding information on the Internet – There is published information about you on the Internet. You can do a search to see what is there.
- Finding information in public records – Many state and local governments have our personal information in public records, some of which can be accessed online.
- Dumpster diving – All too often, we throw personal information in the trash – preapproved credit card applications, account statements, etc. Unfortunately, at times, businesses and other organizations have thrown away records containing personal information.
- Fake IDs – Creation and use of fake IDs. This involves something as simple as using a computer and a color printer. There are sites on the Internet that specialize in the creation of fake IDs.

- Mail theft – Personal information is contained in both incoming and outgoing mail, making unprotected mail prone to theft.
- Using false pretenses – Many schemes succeed because people are too trusting. Common techniques that are used to steal personal information include:
  - Credit card skimming – Using a special device to copy the magnetic information on a card, and then creating a duplicate card. This can happen when someone takes your card out of sight (e.g. – a restaurant).
  - Phone schemes – Calling and impersonating something legitimate to get you to divulge personal information.
  - E-mail schemes – Sending fake e-mails (see phishing below) with links or phone numbers designed to get you to divulge personal information.
- Shoulder surfing at ATMs or public Internet terminals – Someone looking over your shoulder to obtain passwords and/or PINs.
- Insider theft – Theft of files and records by business and/or government insiders.



Things You Should Do: Deter, Detect and Defend

Here is a list of specific things you can do to protect yourself.

Deter

- Protect your purse or wallet at all times.
- Empty your wallet/purse of extra credit cards, IDs, and your Social Security card
- Memorize your SSN and all your passwords.
- Promptly remove mail from your mail box. Deposit outgoing mail only in post office collection mail boxes or at your local post office. Do not leave in unsecured mail receptacles.
- Opt out of pre-approved credit cards. Call 888-5-OPTOUT (888-567-8688) or go to **https://www.optoutprescreen.com/?rf=t** to sign up online.
- Never put account numbers on post cards or on the outside of an envelope
- When you reorder checks have them delivered to your financial institution and pick them up instead of having them mailed to your home.
- Don't put your full name on checks. Use initials only.
- Be sure your checks are endorsed by your financial institution and incorporate security features that help combat counterfeiting and alteration. Checks purchased from EECU do contain special security features to protect you.
- Pay bills online using EECU's bill pay, instead of mailing them.
- Do a search of your name on the Internet to see if any personal information is available.
- Buy a shredder and use it to shred pre-approved credit card applications, credit card receipts, bills and other financial information you don't want.
- Never leave receipts at bank machines, bank windows, trash receptacles, or gasoline pumps.
- Never give personal information over the telephone unless you initiated the call and can positively identify the other party.
- Give businesses only the minimum, essential personal information.
- Sign all new credit cards or add "ask for ID."
- Notify credit card companies and financial institutions in advance of any change of address or phone number.

- Never loan your credit cards to anyone else.
- Beware of solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit / debit card information.
- Do not be afraid to challenge any request for personal information.
- Pay attention to who is around you when using ATMs.
- If someone pays you with a cashier's check, have them accompany you to cash it if possible.
- Consider putting a PIN on your credit. See details at **http://www.consumersunion.org/pdf/security/securityTX.pdf**

Deter - Internet Perspective

Protect your passwords.

Maintain control of your passwords with these simple suggestions:

- Do not write passwords down.
- Do not give passwords to anyone else – ever.
- Watch out for shoulder surfing.
- Use complex passwords, something not in a dictionary. Use a combination of letters and numbers, and at least one capital letter. To help remember your password, modify a word such as "money" by substituting some of the letters. You can change an O to 0, and an E to 3. Money would become M0n3y. Other possible substitutions could include @ for A, 1 or ! for L.
- Change passwords periodically.
- Disable Windows automatic password entry – See **http://www.itistudy.com/autocomplete.asp**.
- When subscribing to an online service, check out the company before giving them personal information. Use a payment intermediary (e.g. – PayPal) when possible. Be sure to read and understand their Privacy Policy. Finally, watch for con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number you used to subscribe.

Keep your PC safe.

New security issues are discovered daily. Some security issues allow an attacker to take over your PC. Some can result in vital files being deleted. Some can install keyloggers to capture your keystrokes, including login IDs and passwords. Suggestions to follow:

- Apply security updates as soon as possible.
- Upgrade your browser to the latest version.
- Keep Windows privacy setting at medium high or higher.
- Have Windows block popups and only allow from specific, trusted sites (e.g. Bill Pay).
- Install antivirus and antispyware, and keep the definitions current.
  - ✓ MacAfee – Available at most retail stores selling software.
  - ✓ Norton – Available at most retail stores selling software.
  - ✓ TrendMicro – Available at most retail stores selling software.
  - ✓ Grisoft – You can get a free version for personal use at **http://free.avg.com**
- Antispyware:
  - ✓ Adaware – lavasoft.com (choose free Adaware Personal Edition).
  - ✓ Spybot – spybot.com/en/download/index.html.

- ✓ Windows Defender – **www.microsoft.com/athome/security/spyware/software/default.mspx**
- If spam is a problem, consider a security suite from one of the antivirus vendors.

Avoid e-mail threats.
Many email threats are circulating on the Internet: These include phishing (see What is Phishing); voice Phishing or Vishing (see What is Vishing); fake multifactor authentication (MFA) notices; Canadian lottery and Nigerian scams (promise large amounts of money, but require you to send them money for taxes, etc.); viruses and worms in e-mail attachments; and other unsolicited "too good to be true" offers. Specific recommendations include:

- Don't click on links in e-mails where you don't know the sender. Look for obvious spelling or grammatical errors in emails from unknown senders. Many come from foreign countries and have multiple errors indicating the sender is not fluent in English.
- Don't post your e-mail address on the Internet, or if you do, use an alternate address (e.g. – Yahoo or Hotmail). This exposes you to spam lists.
- Don't open attachments from unknown senders. They could contain worms or viruses.
- Don't believe or respond to "too good to be true" offers.
- Use caution when disclosing account numbers, credit card numbers, or other personal financial data at any website or online service location. Check to make sure it is a secure site (https instead of http).

Avoid other threats.
When buying online or subscribing to an online service:

- Check out the company.
- Use an intermediary for payment when possible (e.g. – PayPal).
- Read and understand the Privacy Policy.
- Watch out for follow-up e-mails asking for confirmation.

Detect

The following are some suggestions for detecting Identity Theft.

- Reconcile your monthly bank statement within 30 days of receipt in order to detect any unusual activity or unauthorized purchases.
- Be conscious of normal receipt of mail. Contact senders or the US Postal Service if mail is not arriving as it should.
- Order your credit report from the three credit bureaus once a year to check for discrepancies (if married, order your spouse's credit report also). To do this, visit **www.annualcreditreport.com** or **www.ftc.gov/credit**; call 877-322-8228; or write to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- Run regular scans of your PC for viruses and spyware.
- Check out suspicious e-mails and answering machine messages/voicemails. If there is any doubt about the authenticity, contact your financial institution. The following are legitimate 800 numbers for EECU Members:
  - 817-882-0800: EECU Member Services (local number).
  - 817-882-XXXX: Other EECU local numbers.
  - 817-594-XXXX: We have a few numbers for local access by Weatherford Members that otherwise must make a long distance call.

- 800-333-9934: EECU Member Services (for calls outside the local area).
- 800-442-4757: Credit card account information.
- 800-337-3392: Credit card security monitoring service. Members may get a call from or may have a message to call this number about a questionable credit or debit card transaction.

- If your financial institution offers e-mail or text message alerts, sign up for them. EECU Members can, for example, get messages telling them someone has signed into their account, used their debit card, made an electronic withdrawal from their account, etc.

Defend

If you become a victim, be prepared to spend many hours getting matters resolved. Here are specific things to do and related contact information:

- Contact EECU – 817-882-0800 (local) or 800-333-9934, extension 800 (out of the local area) to report if your EECU debit card is lost or stolen.
- If your EECU credit cards are lost or stolen, you can report the loss 24/7 by calling 800-442-4757. Most other card companies also have a 24-hour emergency service phone number.
- File a claim with the FTC at **www.consumer.gov/idtheft**; you can also call 877-FTC-HELP or 877- ID-THEFT. You should also complete an **ID Theft Affidavit** to provide to each creditor.
- Contact all creditors, by phone and in writing, to inform them of the problem.
  - Call your nearest Postal Inspection Service office. Their Fraud Hotline is 800-269-0271 or you can go to http://usps.com/postalinspectors
- File a police report.
- Call each of the three credit bureau's fraud units to report identity theft and ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts.

  Equifax
  P.O. Box 105873, Atlanta, GA 30348-5873
  Telephone: 1-800-997-2493

  Experian Information Solutions (Formerly TRW)
  P.O. Box 949, Allen, TX 75013-0949
  Telephone: 1-800-397-3742

  TransUnion
  P.O. Box 390. Springfield, PA 19064-0390
  Telephone: 1-800-916-8800

- Alert other financial institutions to flag your accounts and to contact you to confirm unusual activity.
- Close compromised accounts and reopen new ones. At EECU, we have an automated process to make this as easy as possible.
- Request a change of PIN for ATM and audio response systems.
- Request a change of password for Online Banking systems.
- Contact the Social Security Administration's Fraud Hotline.
- Contact the state office of the Department of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.

- Keep a log of all contacts and make copies of all documents.
- You may also wish to contact a privacy or consumer advocacy group.

Other Important Contacts

- Looks Too Good To Be True
  - http://www.lookstoogoodtobetrue.com
- Consumer Privacy Guide
  - http://www.consumerprivacyguide.org
- Identity Theft: Prevention & Survival
  - http://www.identitytheft.org
- Privacy Rights Clearinghouse
  - http://www.privacyrights.org/identity.htm

Other Related Information

What is Phishing? A new type of e-mail scam known as "phishing" is rapidly becoming a security risk for computer users. Phishing happens when someone attempts to steal personal information from you by sending you a fraudulent e-mail, claiming to be an organization with which you have some type of relationship (i.e. online merchants, online financial institutions, etc.)

The e-mail or phone message often has a sense of urgency, telling consumers to “act immediately,” or it will contain directives to confirm personal or account information. Often these e-mails will threaten to “cut off services” if account information is not verified.

E-mail scams will often ask for personal or account information, such as:

- Account numbers
- Credit and debit/check card numbers
- Social Security numbers
- Internet Banking user-IDs and passwords
- Mother's maiden name
- Date of birth
- Other sensitive information

Fraudulent e-mails often include links that contain the names or web addresses of legitimate companies. Additionally, these e-mails will disguise or forge the sender's e-mail address so they appear to be legitimate.

Phishing e-mails usually provide a link to a website and generally tell you that it's time to update your personal information or that they have upgraded their servers and need you to re-enter your personal information. That personal information might be a username, password, credit card number, and maybe even your home address or phone number. The link in the e-mail goes to a site that has a similar look and feel (perhaps even a logo) to the site they are imitating, as well as a similar web address.

In the past, some EECU Members received a fraudulent e-mail that appeared to be from EECU asking for personal account information. If you receive such an e-mail, DO NOT OPEN THE ATTACHMENT or click on any links in the e-mail. Opening the attachments or clicking on any links could potentially infect your computer with a malicious program and jeopardize the security of your personal information.

There are many variations of phishing. One variation involves sending you an e-mail from a company you do not recognize, which provides a link to a website that is selling something. You then give a credit card number, thinking you are buying something, but the whole site ends up being a big scam created just to collect credit card numbers. Another variation is that the e-mail appears to come from the government and claims you will lose your federal insurance coverage on your savings and checking account unless you update your records on their site (you can read more about this variation **on the FBI website**.

EECU does not send our Members e-mails asking for personal information such as your Credit Union username, password, pin number, or other personal identity information. EECU will use personal information from your account to verify your identity if you call us, but we will NEVER call you and ask you to give personal or account information over the phone. If this happens, get the name and phone number of the person and then **contact Member Services** (817-882-0800).

Click here to see a copy of a fraudulent e-mail.

What is Vishing? Voice phishing or vishing attempts to extract personal information from Credit Union Members by having them call a bogus phone number (usually an 800 number). When they call, a live person answers and requests identifying information. This often includes requests for account numbers, debit card numbers and PINs, and the like. The vishing request can arrive via regular mail, e-mail, or in the form of a message left on an answering machine. There is typically some sort of urgency to the message, such as the account will be deactivated if they do not call.

To avoid being victimized by this scam, Members should only call specific numbers unique to the Credit Union. The following are legitimate 800 numbers for EECU Members:

- 817-882-0800: EECU Member Services (local number).
- 817-882-XXXX: Other EECU local numbers.
- 817-594-XXXX: We have a few numbers for local access by Weatherford Members who otherwise must make a long distance call.
- 800-333-9934: EECU Member Services (for calls outside the local area).
- 800-442-4757: Credit card account information.
- 800-337-3392: Credit card security monitoring service. Members may get a call from or may have a message to call this number about a questionable credit or debit card transaction.

Return to eecu.org