Prevention

Tips

McCoy Federal

Your Full-Service Community Credit Union

Security Threats & Prevention Tips

WHAT IS IDENTIFY THEFT?

Identify theft occurs when someone uses your name or personal information, such as your Social Security number, driver's license number, credit card number, telephone number or other account numbers, without your permission. Identity thieves use this information to open credit accounts, bank accounts, telephone service accounts, and make major purchases – all in your name. Information can be used to take over your existing accounts, or to open new accounts. Identity theft can result in damage to your credit rating and denials of credit and job offers.

HOW DOES IDENTITY THEFT HAPPEN?

Identity theft commonly begins with the loss or theft of a wallet or purse. But there are many other ways that criminals can get and use your personal information in order to commit identity theft.

The following are some examples:

Example #1 - One evening you sit down to pay your monthly bills. You write the checks, toss the statements in the trash and put the container out on the curb for the morning's trash pick-up. While you sleep, "dumpster-divers" go through your trash looking for the papers you've thrown away. They discover a gold mine of information that can be used for fraudulent purposes - your name, address, phone number, utility service account numbers, credit card numbers, and your Social Security number.

Example #2 - You receive an email message from what appears to be your Internet Service Provider (ISP). The message requests that you update the information they have on file about you – your name, credit card number, bank account number, etc. – by replying to the email or going to a specific Web site address to provide the information. However, neither the message nor the Web site address is from your ISP. They belong to someone who wants to get your information to steal your identity.

PROTECT YOUR IDENTITY

- ✔ While there is no guarantee that your identity will never be stolen, there are steps you can take to minimize the risk:
- ✔ Do not give out your Social Security number to people or companies that you do not know.
- ✔ Before disclosing any personal information, make sure you know why it is required and how it will be used.
- ✔ Shred information you no longer need that contains personally identifiable information and account numbers. For example, credit card receipts, billing statements and pre-approved credit offers should be shredded before you discard them.
- ✔ Guard your mail from theft. Promptly remove your incoming mail from your mailbox and place outgoing mail in post office collection boxes. Install a locking mailbox if mail theft is a problem in your neighborhood.
- ✔ Keep the personal information you have at home and at work in a safe place.
- ✔ Do not carry extra credit cards, your birth certificate or passport, or other cards that display your Social Security number in your wallet or purse, except when necessary.
- ✔ Create unique passwords and personal identification numbers (PINS) and avoid using easily available information such as mother's maiden name, date of birth, or the last four digits of your Social Security number. Use passwords on your banking and brokerage accounts.
- ✔ Get a copy of your credit report from each of the three major credit reporting agencies at least once a year. Review the reports to be sure no one else is using your identity to open new accounts or not use your existing accounts.

IF YOU'RE A VICTIM

- ✔ Contact the fraud departments of the three major credit bureaus. Request that a "fraud alert" be placed on your file and include a statement that creditors must get your permission before any new accounts are opened in your name. Get a copy of your credit report from each credit bureau so that you can dispute any inaccurate information Check your reports at least every six months. You can contact the three major credit bureaus at the following:
  - **EQUIFAX**, www.equifax.com - Order Credit Report: 800-685-1111
    Report Fraud: 800-525-6285
  - **EXPERIAN**, www.experian.com - Order Credit Report: 888-397-3742
    Report Fraud: 888-397-3742
  - **TRANS UNION**, www.tuc.com - Order Credit Report: 800-888-4213
    Report Fraud: 800-680-7289
- ✔ Contact all the creditors involved. Let them know that your accounts may have been used without your permission, or that new accounts have been opened in your name. If your accounts have been used fraudulently, ask that new cards and account numbers be issued to you. Check your billing statements carefully and report any fraudulent activity immediately. Many banks and creditors will accept the "ID Theft Affidavit" available at www.consumer.gov/idtheft, to dispute the fraudulent charges.
- ✔ File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- ✔ Contact the Federal Trade Commission. The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); by mail, Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580; or online at www.consumer.gov/idtheft. Also request a copy of the publication, "ID Theft, When Bad Things Happen to Your Good Name."
- ✔ Keep a record of your contacts. Start a file with copies of your credit reports, the police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties. Follow up all phone calls in writing and send all correspondence certified, return receipt requested.

ADDITIONAL RESOURCES

Non-Profit Organizations

Privacy Rights Clearinghouse, 3100 5th Ave., Suite B, San Diego, CA 92103 / 619-298-3396 /
Email: prc@privacyrights.org / www.privacyrights.org
Identify Theft Resource Center, P.O. Box 36833, San Diego, CA 92196 / Email: voices123@att.net /
www.idtheftcenter.org

Federal Government Agencies

Federal Bureau of Investigation / www.fbi.gov/contact/fo/norfolk/ident.htm
FBI Internet Fraud Complaint Center / www.ifccfbi.gov
Federal Trade Commission, Identify Theft Clearinghouse, 600 Pennsylvania Ave., N.W., Washington, DC 20580
1-877-IDTHEFT (438-4338) / www.consumer.gov/idtheft
Social Security Administration, SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235 / 1-800-269-0271 /
email: oig.hotline@ssa.gov
U.S. Postal Inspection Service / www.usps.gov/websites/depart/inspect

State & Local Government Agencies

Contact your State Attorney General's office or local consumer protection agency to find out whether your state has laws related to identify theft.

IDENTIFY THEFT PREVENTION TIPS:

- ✔ Safeguard your personal information.
- ✔ Do not share personal information with unknown person or companies.
- ✔ Carry with you only the information you need.
- ✔ Order and review a copy of your credit report at least once a year.
- ✔ Shred documents containing sensitive information before discarding.

IF YOU BECOME A VICTIM:

- ✔ Contact McCoy Federal Credit Union fraud department
- ✔ Contact all the creditors involved.
- ✔ File a police report.
- ✔ Contact the Federal Trade Commission.

FREE Credit Reports

You are eligible to one free credit report every 12 months from each of the nationwide consumer credit reporting companies: Equifax, Experian and TransUnion. Monitoring and periodically reviewing your credit report is an effective tool in fighting identity theft.

Request your Credit Report Online
Visit: **www.annualcreditreport.com**
You can see and print your report online. It's quick, easy and secure.

Request your Credit Report by Phone
Call (toll free): 877-322-8228. You will go through a simple verification process over the phone. Your reports will be mailed to you.

Request your Credit Report by Mail
You can request your credit report by mail by filling out the **request form**
(to download, go to: www.annualcreditreport.com/cra/order?mail)
Mail the completed request form to: Annual Credit Report Request Service
P.O. Box 105281 Atlanta, GA 30348-5281

For your security, and in order to ensure you are using the request form that has been authorized by the Central Source, please use the link above to download the form from this website. Only the Central Source, Equifax (www.equifax.com), Experian (www.experian.com) and TransUnion (www.transunion.com) as it's members, have been authorized by law and the government (see FTC.gov) to provide free credit reports per the FACT Act.
Do not provide your personal information to persons not authorized or listed above.

FBI FRAUD ALERT

Don't Get Ripped Off!

IF YOU CAN ANSWER "YES" TO ANY OF THE FOLLOWING QUESTIONS, YOU COULD BE INVOLVED IN A FRAUD OR ABOUT TO BE SCAMMED!

- ✔ Is the CHECK from an item you sold on the internet, such as a car, boat, jewelry, etc?
- ✔ Is the amount of the CHECK more than the item's selling price?
- ✔ Did you receive the CHECK via an overnight delivery service?
- ✔ Is the CHECK connected to communicating with someone by email?
- ✔ Are you receiving PAY or a COMMISSION for facilitating money transfers through your account?
- ✔ Have you been asked to PAY money to receive a deposit from another country such as Canada, England, or Nigeria?
- ✔ Have you been instructed to either "WIRE", "SEND", OR "SHIP" MONEY, as soon as possible, to a large U.S. city or to another country, such as Canada, England, or Nigeria?
- ✔ Have you been informed that you were the winner of a LOTTERY, such as Canadian, Australian, El Gordo, or El Mundo, that you did not enter?
- ✔ Is the CHECK drawn on a business or individual account that is different from the person buying your item or product?
- ✔ Did you respond to an email requesting you to CONFIRM, UPDATE, OR PROVIDE your account information?

If you suspect fraudulent activity -please contact us immediately!

Types of Account Fraud include Checking, Credit Card, ATM, Identity Theft, Electronic

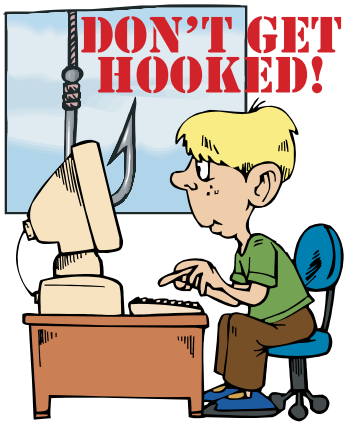
Account fraud is one of the fastest growing crimes in the nation. McCoy Federal has safeguards to help prevent and detect account fraud, but it is YOUR knowledge, awareness and alertness that are the most important first lines of defense in preventing fraud.

Minimize Your Risks to Prevent Fraud

- Protect your account & personal information - never respond to unsolicited requests for this information, whether it's over the phone, through the mail or via the internet.
- Online, only provide your credit card number on a secure web page, which is identified by the small lock icon (& is locked) displayed in the lower right corner of the browser.
- Use a single credit card, with low credit limit, for internet purchases.
- Do Not Send credit card information via e-mail or instant messenger - neither are secure.
- Do Not Have confidential information preprinted on your checks.
- Report any lost or stolen credit cards or checks to the issuing institution immediately.
- Shred any documents containing confidential information, including unused checks (even if the account was closed), ATM receipts and old credit card receipts, before disposal.
- Review all account and credit card statements once they are received to determine that no account irregularities are apparent.
- Notify your credit union if newly ordered checks or your regular statements do not arrive in a timely manner. A missing statement may mean someone has changed your billing address to prevent you from seeing fraudulent transactions.
- Deposit outgoing mail directly into post office boxes, not in your own mailbox. If you are going on vacation, place a delivery hold on your mail.
- Carry a minimum number of ID and credit cards. Do not carry your social security card, PIN numbers or passwords in your wallet or purse and make copies of all items that you do carry.
- Cancel and destroy any credit cards that you don't need or use. View your credit report at least once a year.

Did You Know...

You are personally responsible for the checks and money orders you deposit, not the financial institution. This is because you are in the best position to determine how risky the transaction is since you are dealing directly with the person issuing the payment.



Caution! Thieves are "phishing" for your information...
What is Phishing? Phishing attacks use 'spoofed' emails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security numbers, etc. By hijacking the trusted brands of well-known financial institutions, online retailers and credit card companies, phishers are able to convince many recipients to provide personal andfinancial information.

How You Can Avoid Phishing Scams
The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe as a general rule, you should be careful about giving out your personal financial information over the Internet.

The Anti-Phishing Working Group (www.antiphishing.org) has compiled a list of recommendations that you can use to avoid becoming a victim of these scams.

- ✔ Be suspicious of any email with urgent requests for personal financial information.
- ✔ Don't use the links in an email to get to any web page, if you suspect the message might not be authentic.
- ✔ Avoid filling out forms in email messages that ask for personal financial information.
- ✔ Always ensure that you're using a secure web site when submitting credit card or other sensitive information via your Web browser.
- ✔ Regularly log into your online accounts and check your financial, credit and debit card statements to ensure that all transactions are legitimate.

Always report phishing or spoofed emails by forwarding them to:

1. reportphishing@antiphishing.com & spam@uce.gov
   Forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
2. When forwarding spoofed messages, always include the entire original email with its original header information intact.
3. Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their web site: www.ifccfbi.gov/

If you've given out your personal financial information:
Visit http://www.antiphishing.org/consumer_recs2.html for some tips on what to do if you have given out any personal information.

The **Anti-Phishing Working Group (APWG)** is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For up to date information and the latest phishing scams, visit their site at: **www.antiphishing.org**

Resources

Identify Theft Resource Center
www.idtheftcenter.org
Identity Theft - Federal Trade Commission
www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm
Federal Bureau of Investigation
www.fbi.gov/contact/fo/norfolk/ident.htm
FBI Internet Fraud Complaint Center
www.ifccfbi.gov
Federal Trade Commission, Identify Theft Clearinghouse
www.consumer.gov/idtheft
National Fraud Information Center
www.fraud.org
Anti-Phishing Working Group
www.antiphishing.org
Spam - Federal Trade Commission
www.ftc.gov/spam/
Annual Credit Report.com
www.annualcreditreport.com/cra/index.jsp
Equifax
www.equifax.com
Experian
www.experian.com
TransUnion
www.transunion.com