

EMAIL SCAMS (PHISHING)

If you get an email or pop-up message that asks for personal or financial information, do not reply and do not click on any links! Most companies will not ask for this information by email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number that you know to be genuine.

Don't email personal or financial information.

Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

Be cautious about opening any attachments, links or downloading any files from emails or Instant Messages (IM's) that you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

If you believe you've been scammed, file your complaint at www.ftc.gov. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. Call your bank or credit card company for more information.

RESTORING YOUR CREDIT

Protect your credit report:

Add a fraud alert to your credit file to warn potential credit grantors that you may be a victim of ID Theft.

Obtain and review a copy of your credit report:

Periodically check for any unauthorized activity on your credit report. Should any information not pertaining to you show up on your credit file, contact the creditors and question the account and/or inquiry. If you have questions, contact TransUnion and/or the other major credit reporting companies.

Report the fraud:

Contact government agencies such as the Federal Trade Commission (FTC) to report the fraudulent activity. It is recommended that you also contact your local law enforcement agency to file a report regarding the fraudulent activity.

Contact your credit financial institutions:

Contact companies that you have relationships with and inform them that your accounts with those companies may be compromised. Contact the companies on your credit report that you do not recognize. Verify with the company, the information they have in their records for the reported item. Provide the creditor with a copy of your police report, notarized FTC Affidavit or other relevant documentation. Keep a log of all related phone conversations, including names of people with whom you spoke.

Checks and Social Security number:

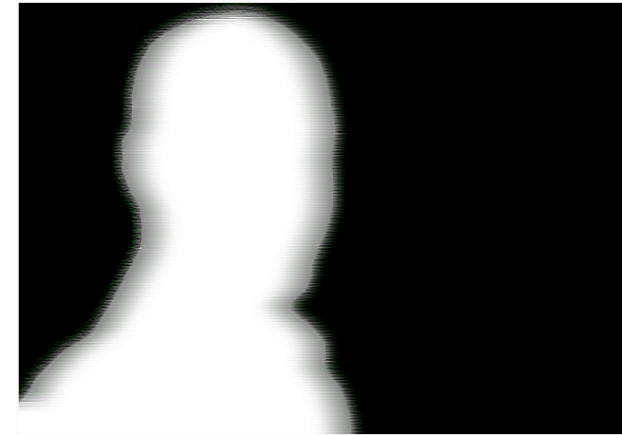
Notify your bank to stop checks. You can also report stolen checks by filing a complaint with the United States Social Security Administration. www.ssa.gov

Follow up:

Follow up with companies and agencies that you have contacted to ensure that their investigation resulted in your favor. Remember that the victim has certain responsibilities. By working with credit grantors directly to identify all fraudulent accounts, you can greatly reduce the effects. Periodically review your credit report for any new fraudulent activity.

Information provided by: www.transunion.com

IDTHEFT / FRAUD MINIMIZE YOUR CHANCES OF BEING A VICTIM



**Information
Security
Office**

Provided for faculty, staff and students by:

*The University of Texas at Arlington
Office of Information Technology (OIT)
Information Security Office*

www.uta.edu/security
security@uta.edu
817.272.5487

Available in accessible format on website

(Revised: 05/30/08, Information Security security@uta.edu)

Purpose of this Brochure

Identity Theft is quickly becoming a common occurrence in today's world. Many say that it is not a matter of "if" but just a matter of "when" a person will have their identity stolen. You have potentially shared your financial information with hundreds of institutions and anyone of them is at risk of a data compromise. Some will report it while others will try to avoid the issue putting you at an increased risk of identity fraud. Here are a few steps you can take to minimize the risks.

SIGNS THAT YOU MAY BE A VICTIM

- One of your creditors informs you that they have received an application for credit.
- Calls or letters state that you have been approved or denied by an unknown creditor.
- You receive bills in your name and address for services for which you never applied.
- You no longer receive your credit card statements, or notice mail not being delivered.
- Your credit card statement includes unusual purchases that you don't remember making.
- Collection agencies are contacting you for an account established with your identity.

Information provided by: www.transunion.com

TAKE ACTION AGAINST ID THEFT / FRAUD

- Report the incident to the police immediately.
- Report stolen cards to issuers immediately.
- Notify your bank if your checks were stolen, and close your account and open a new one.
- Be prepared to fill out FTC affidavits of forgery to establish your innocence.
- If you use an ATM card for banking services get a new card.
- Contact TransUnion to place a fraud alert on your credit file. Ph: 800-680-7289.

Information provided by: www.transunion.com

CREDIT CARD / BANK CARD SECURITY

Fraudulent manufacturing of credit cards and bank cards is on the rise. It is becoming increasingly easier for criminals to create fake cards that allow them access to your money. They often obtain the information needed to make these cards through stolen financial records from retailers or institutions that have your card information in a database. Here are some tips that may slow criminals down providing you valuable time to cancel cards.

Use Check ID instead of Signature: Where it asks for a signature on the back of your credit or bank card write "Check ID" instead of your name. A lot of retailers with a keen eye will see this and ask for your drivers license for further verification.

Know your cards: Go through your cards and make a list of the names and contact numbers for each. Keep this list in a safe place. If you ever lose or have your wallet stolen you will have the information you need to quickly cancel the cards. Always review your card activity listed in the monthly statements.

Carry one card: It is convenient to have all your credit cards in your wallet but this makes it easier for a criminal who has stolen your wallet or purse to rack up a lot of charges quickly. When possible carry one card with you and leave the others hidden in a safe place. Also, if you don't plan to do a lot of shopping, carry a card that has a low spending limit.

Use Credit instead of Debit Bank Cards: In most cases using a credit card is safer than using a debit bank card. Most credit cards will not charge you a penalty if your card is used fraudulently (Check your credit card contract for details). Also, using a debit bank card may put you at risk of your data being intercepted from a retailers database electronically, giving criminals direct access to your bank account. Periodically review your bank accounts and your credit report (call your bank for more information).

Card Receipts: Shred your credit card and debit card receipts if you plan to discard them in the trash.

Use a secured locking mailbox or consider a Post Office Box. Pick up all ordered checks at your bank!

FLAGGING YOUR CREDIT ACCOUNT

If you are a victim of identity fraud you can place an extended seven year credit alert on your credit file. If someone tries to take out a line of credit in your name the issuer will see that there has been an alert issued. The issuer will often try to contact you at a phone number that you can designate during your credit alert enrollment. Tip: You may want to use your cell phone number for your call back number so that you can be contacted immediately!

In order to place an extended alert on your file that lasts seven years you will have to report the identity fraud incident to the police. You may be asked to provide a case number by the reporting agencies assigning the alert to your credit file.

However, if you suspect that you may be a victim of identity theft, or just want to be extra cautious, you can place a temporary (90 day) initial fraud alert on your credit report and if necessary re-issue the alert every 90 days. Tip: Mark your calendar!

Remember that having an alert on your account means that you may have to temporarily remove the alert anytime you want to check your credit report or obtain a line of credit. Do this by contacting the reporting agency with whom you filed the alert.

When you request an alert from one agency it is practice for them to notify the other agencies. You should within two weeks receive letters from all three. Keep these letters on file so that if there is an issue with a creditor you have proof of the alert.

REPORTING ID THEFT / FRAUD

Contact numbers for credit reporting agencies:

- TransUnion: 800-680-7289 www.transunion.com
- Equifax: 800-525-6285 www.equifax.com
- Experian: 888-397-3742 www.experian.com
- FTC: 877-ID-THEFT www.ftc.gov/idtheft

Receive a free copy of your credit report at:
www.annualcreditreport.com