Protecting Yourself Against Identity Theft

This program is made possible by a grant from the FINRA Investor Education Foundation through Smart Investing@your library®, a partnership with the American Library Association.
What is Identity Theft?

• Identity theft is when someone uses your personal information without your knowledge or permission to commit fraud. Usually for their financial gain.

• Social Security number theft is the top theft type reported in Utah.
Who Does it Affect

17.6 million identity theft victims in 2014 (7% of US population)*

Nearly 500,000 complaints to the FTC in 2015.

*U.S. Dept. of Justice, Bureau of Justice Statistics, Victims of Identity Theft, 2014 (September 2015)
Types of Identity Theft

• Tax Identity Theft:
  – Uses a stolen Social Security number to claim a false tax return.

• Child Identity Theft:
  – Usually occurs through a stolen Social Security number.

• Medical Identity Theft:
  – Stolen personal information is used to obtain medical care.
What More can Identity Thieves Do?

- Open new utility accounts in your name.
- Open credit cards in your name.
- Give your name when they are arrested.
RECOGNIZING IDENTITY THEFT
Warning Signs

- Withdrawals on your bank account that are not yours.
- You have unfamiliar accounts on your credit report.
- Your credit cards are declined at stores.
- You do not receive bills in the mail.
- Receive bills from a doctor that are not yours.
- Problems with filing your tax return.
  - The IRS already has your return on file.
How Do They Get Your Information?

- Criminals hacking into ATM’s or other credit card readers.
- Fake charitable organizations asking for money.
- Scam artists posing as utility service agents trying to obtain money.
- Criminals posing as IRS agents requesting personal information.
- ”Phishing” emails with false links attached.
- Off-Shore scams.
Be Cautious of...

- Computer pop-ups telling you to buy anti-virus software.
- Phone calls, texts messages, or emails asking for personal information.
- Suspicious links attached to emails.
- Emails stating you could receive large amounts of money.
Spotting a Scam

Dear Visa customer,

This email is to inform you of a recent update we made to our systems, To avoid service interruption we require that you confirm your account as soon as possible.

Please take a moment to confirm your account by going to the following address:

http://visa-secure.com/personal/secure_with_visa/

Follow these steps:

1: Confirm your account by clicking the link above.
2: Verify your visa card information.
3: Your account will then be updated, you may continue using your visa without any in

*** Please note: If you FAIL to update your visa card, it will be temporarily disabled.

We apologize for any inconvenience this may cause. The visa team is working hard to bring you the best services on the web.
Spotting a Scam

From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530

Dear Email User,

This is to inform you that on 4th February, 2015, Microsoft Outlook will discontinue support on your account and security. If you choose not to update your account on or before 4th February, 2015, you will not be able to read and send emails, and you will no longer have access to many of the latest features for improved conversations, contacts, and attachments.

Update Your Account

Take a minute to update your account for a faster, safer, and full-featured Microsoft Outlook experience.
Thank You
Outlook Warning! Member Service
WHAT IF YOU BECOME A VICTIM OF IDENTITY THEFT?
Report Fraud

• File a police report.
• Change all account passwords.
• Fill out the Identity Theft report on the Federal Trade Commission website.
• Fill out the Identity Theft Report at IRIS if you live in Utah. www.idtheft.utah.gov
Reporting Fraud (Continued)

- Contact your bank, credit card companies, utility companies.
- Get a new drivers license.
- Place a fraud alert on your credit reports.
  - This stays on for 90 days and alerts creditors that you suspect you are a victim of fraud.
  - The creditor should take extra precautions if they issue credit in your name.
  - You just need to file one fraud alert and they will contact the other two credit reporting agencies.
Credit Report Security Freeze

• Permanent hold on your credit.
• $10.00 to place the freeze.
• You can temporarily remove the freeze for $10.00
• Designed to protect your identity.
  – Prevents credit, loans, and financial services from being approved without your consent.
IdentityTheft.gov Helps You Report and Recover from Identity theft
Tell us what happened.  
Get a recovery plan.  
Put your plan into action.
### FREE help from IdentityTheft.gov

- **Get a personal recovery plan** that walks you through each step.

- Create an **identity theft affidavit** that you can review and update at any time.

- Get **customized pre-filled letters** to send to credit bureaus, businesses, and debt collectors.

- Return anytime to **update your plan** and **track your progress**.

- Get advice about what to do if you’re affected by **specific data breaches**.
Prevent More Fraud From Occurring

• Notify your creditors or banks where the fraudulent activity occurred.
  – Closing your accounts should be a top priority
  – Report any fraudulent activity as soon as you are aware of it.
  – Fair Credit Billing Act specifies that the most you have to pay for unauthorized charges is $50.
PROTECTING YOURSELF
Keeping Your Identity Safe

- Shred documents with personal information.
- Know your payment due dates.
- Read credit card statements carefully and often.
- Read your health insurance plan statements.
- Review each of your credit reports once a year.
Protecting Sensitive Information

• Lock up your important papers.
  – Social Security, I-9 forms, VISAs, Passports, Marriage License.
• Make sure to report stolen credit cards or driver license immediately.
• Do not carry your Social Security Card in your purse or wallet.
• Do not give any personal information to anyone via phone, text, or email unless you initiated the contact.
Protecting Your Children

Child Identity Protection (CIP) program:

• Prevent Identity Thieves from opening credit under a child’s name.

• Places the child’s information in a High Risk Fraud database.

• The information will remain in the database until the child is 17.

  – Verify you are the parent/guardian
  – Enter your child’s information
  – Submit the information
Protecting Your Children

• Contact all three credit reporting companies and report the situation.

• File a police report with your local law enforcement agency.

• File a complaint with the CFPB at help.consumerfinance.gov/app/creditreporting/ask.

• When you contact the credit reporting companies, provide the following information about the child:
  – Legal name
  – Address
  – Birth date
  – A copy of the child's birth certificate
  – A copy of the child's Social Security card

• And information about yourself:
  – A copy of your driver's license or other government-issued identity card with your current address
  – A copy of a current utility bill
Watch Your Credit

• Check your credit reports, three times a year.
• Contact credit reporting agencies.
• Put a fraud alert on your credit report.
• Consider putting a credit freeze on your reports.
Free Access to Your Credit Reports

www.annualcreditreport.com

Phone: 1-877-322-8228

Write: Annual Credit Report Request Service
P.O. Box 105281 Atlanta, GA 30348-5281
www.annualcreditreport.com

Don't be fooled by look-alikes.

Lots of sites promise credit reports for free. AnnualCreditReport.com is the only official site explicitly directed by Federal law to provide them.

About AnnualCreditReport.com

PLAY   SPOT IDENTITY THEFT   GOOD CREDIT   DON'T BE FOOLEO   MORE THAN A SCORE   NOT LIKE THE OTHERS
Helpful Resources

• Credit Reporting Agencies
  • Equifax - [www.equifax.com/CreditReportAssistance](www.equifax.com/CreditReportAssistance)
  • Experian - [www.experian.com/fraud](www.experian.com/fraud)
  • TransUnion - [www.transunion.com/fraud](www.transunion.com/fraud)
Helpful Website

Websites

– http://idtheft.utah.gov/
– https://www.identitytheft.gov/
– https://www.onguardonline.gov/
Thank you!

This program is made possible by a grant from the FINRA Investor Education Foundation through Smart investing@your library®, a partnership with the American Library Association.