MemberOne
FEDERAL CREDIT UNION

Identity Theft

PARTICIPANT'S GUIDE

Table of Contents

My Identity

What information about me may be shared with others?

Biographical Data	Medical Data	Biometric Data	Financial Data

Common Identity Theft Scams

There are many types of scams that specifically target your identity. Below are some of the most common types of scams. This list is not comprehensive.

Phishing Scams
Definition of phishing: A scam, usually via text message or email, in which a thief pretends to be a legitimate company and tries to get you to give your personal information.

Phishing Email Scams Activity: Change Your Password
Circle or otherwise note anything you find suspicious.

From: YahooMail
Subject: Change your password

Dear Customer,

We notice that you sign in from a different computer. Please log in using this link to verify your password: www.yahooo.com
If you do not verify this information within 24h you account will be permanently deleted.

Best,
Yahoo Team

Phone Scams
Explanation of phone scams: Scammers may make a phone call to a victim and try to sell the victim a product or service that isn't needed. Scammers may use threats or incentives to get the victim to provide the scammers with personal information that they can later use.

Phone Scams Activity: Sweepstakes and Lottery Winners
Circle or otherwise note anything you find suspicious in this phone call.

Hello, Mr. John, you've been specially selected as the winner of our monthly sweepstakes. If you act now, you can collect up to $2 million in cash after taxes. All we need from you is to verify some details, and within a few minutes, the money could be on its way to your bank account. Could you provide your Social Security number for us?

Common Identity Theft Scams, Continued

Elder Fraud Scams
Explanation of elder fraud: Many seniors may own assets such as a house or car and have retirement funds such as a 401(k) or other benefits that can make them an attractive target to identity thieves. Identity thieves may be strangers who try to befriend the senior, a professional who may have access to the senior's home, or even a friend or family member. One of the more common ways in which thieves target seniors is by abusing a power of attorney.

This type of abuse can affect you or your family members, especially if you or one of your loved ones is an older person.

Elder Fraud by Power of Attorney Activity: My Niece, Angela
Circle or otherwise note anything you find suspicious in the actions described here.

Mrs. Garcia was 78 years old when she gave her niece, Angela, power of attorney. Recently, Mrs. Garcia has become quiet and sad. She does not leave the house for her daily walk anymore. Her neighbors noticed that Angela bought an expensive new car and claimed it was for her aunt. Angela is also making plans to remodel and expand the guest bedroom and plans to move in. Since it is her aunt's house, she intends to use her aunt's funds to pay for the expenses. When Angela is not around, Mrs. Garcia complains that some of her things are missing.

Protecting Against Identity Theft

How do you protect your information against identity theft?

Review the list of recommended steps. Put a check by steps that you take already, those you plan to start now, and those you plan to begin doing later.

- Monitor your credit reports and scores*:* Access your credit reports for free at https://www.annualcreditreport.com. You are entitled to one free credit report a year from each of the three main credit bureaus.

  ☐ Already Do ☐ Start Now ☐ Start Later

- Monitor your financial statements: Review financial transactions carefully and correct any errors by contacting the bank or credit card company promptly.

  ☐ Already Do ☐ Start Now ☐ Start Later

- Practice online safety:
  - Log into your email and online banking accounts regularly and change your passwords every few months.

    ☐ Already Do ☐ Start Now ☐ Start Later

  - Use strong passwords that are difficult to guess. Use numbers, punctuation marks, and a combination of capital and lowercase letters.

    ☐ Already Do ☐ Start Now ☐ Start Later

  - Do not click on links or download files from unknown senders, especially files that end in ".exe."

    ☐ Already Do ☐ Start Now ☐ Start Later

  - Become familiar with the language that scammers use to target victims via email.

    ☐ Already Do ☐ Start Now ☐ Start Later

  - Do not use public Wi-Fi to receive or send sensitive documents.

    ☐ Already Do ☐ Start Now ☐ Start Later

Protecting Against Identity Theft, Continued

- Secure your documents:
  - Keep sensitive information in a safe place.

    ☐ Already Do ☐ Start Now ☐ Start Later

  - Do not carry your Social Security card with you.

    ☐ Already Do ☐ Start Now ☐ Start Later

  - Shred sensitive documents once you no longer need them.

    ☐ Already Do ☐ Start Now ☐ Start Later

- Be aware of your surroundings.
  - Cover the ATM keypad when entering your PIN.

    ☐ Already Do ☐ Start Now ☐ Start Later

  - Keep an eye out for “shoulder surfers” who may be watching you key in your phone’s passcode in public spaces.

    ☐ Already Do ☐ Start Now ☐ Start Later

Monitoring Services

- Use a credit monitoring service: Credit monitoring services keep a close watch on your Experian, TransUnion, and Equifax scores, reports, and activity. They can send you updates and alerts based on credit report requests by companies or if a bill is late.

  ☐ Already Do ☐ Start Now ☐ Start Later

- Use an identity monitoring service: Identity monitoring services can fill the gaps credit monitoring services may miss. Identity monitoring services can alert you that your personal information is being used to create accounts or to sign up for services or is showing up in records, such as court records.

  ☐ Already Do ☐ Start Now ☐ Start Later

- Use credit freezes: Credit freezes or security freezes protect your accounts by sealing your credit report off from any agency, organization, or individual who wants to access it until you authorize its release. It can take a few days for the freeze to be lifted if you decide to authorize the inquiry. Requesting a credit freeze or unfreeze to the credit reporting bureaus is free.

  ☐ Already Do ☐ Start Now ☐ Start Later

- Use fraud alerts: Fraud alerts are free and available from any of the three credit reporting bureaus, as long as you provide them with proof of identity. Temporary fraud alerts are free and last up to one year. If you are a victim of identity theft, they can last up to seven years. There are also special packages for those who are deployed in the military.

  ☐ Already Do ☐ Start Now ☐ Start Later

Reporting Identity Theft

If you've become a victim of identity theft, there are a few steps you can take to regain control over your personal information.

STEP 1: Collect Information

- ☐ Review your credit report and monitor any changes caused by the theft.
- ☐ Review the account where the theft occurred and note any changes.
- ☐ Review other and connected accounts.

STEP 2: Report to Fraud Departments and Federal Agencies

- ☐ Report the theft to the fraud department at the organization or company where it occurred. Close all accounts and change all passwords, PINs, and access data to prevent the breach from reoccurring.
- ☐ Report the theft to the three nationwide credit reporting bureaus and request a fraud alert:
    - Experian.com/fraudalert: 1-888-397-3742
    - TransUnion.com/fraud: 1-800-680-7289
    - Equifax.com/CreditReportAssistance: 1-866-349-5191
- ☐ Create an Identity Theft Report by reporting the theft to the Federal Trade Commission
    - Complete the online form at https://www.identitytheft.gov or call 1-877-438-4338. Include as many details as possible.
- ☐ Create a report with the local police.

STEP 3: Repair

- ☐ Review the new accounts created by the thief and close them down.
- ☐ Review and correct statements and charges on your bills, credit reports, and other financial documents.
- ☐ Make a plan of action for monitoring your accounts, or get a paid monitoring service.

The Federal Trade Commission website, https://www.identitytheft.gov, offers free personalized recovery plans.