

MEMBER ID THEFT PREVENTION AND PREPAREDNESS

While you probably can't prevent identity theft entirely, you can minimize your risk.

By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft.

Listed below are several important tips from the FTC's *Take Charge: Fighting Back Against Identity Theft* (formerly: *ID Theft: When Bad Things Happen to Your Good Name*):

- Order a copy of your credit report from each of the three major credit bureaus (Equifax, Experian or TransUnion) at least annually. One free copy can be ordered each year from each credit bureau.
 - Make sure it's accurate, and
 - Includes only those activities you've authorized.
- Place passwords on your credit cards, credit union and phone accounts.
- Secure personal information in your home, especially if you:
 - Have roommates,
 - Employ outside help, or
 - Are having service work done in your home.
- Ask about information security procedures in your workplace.

Other recommended steps:

- Carefully store or dispose of confidential documents.
 - Destroy receipts and old statements in order to keep out of the hands of "dumpster divers."
- Review all account statements promptly. Early detection of ID theft is the key to minimizing loss.
- Use secure mailboxes to send and receive mail.
- Use caution when asked for personal information over the phone, Internet or email.
- Be aware of scam tactics such as "phishing" or "spoofing."
 - Phishing - pronounced like "fishing." The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where the user is asked to update personal information, such as passwords and credit card, social security, and bank account numbers, which the legitimate organization already has. The website, however, is bogus and set up only to steal the user's information.

- Spoofing - email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

- Consider placing a security code on your accounts.

Resources

Publications

- Federal Trade Commission (FTC)
 - *Avoid Credit and Charge Card Fraud*
 - *Facts for Consumers: Electronic Banking*
 - *Tips for Protecting Your Personal Information*
 - *What You Do Know Can Protect You*
 - *ID Theft: What's It All About*
- Federal Deposit Insurance Corporation (FDIC)
 - *Your Wallet: A Loser's Guide*
- Department of Justice
 - *Identity Theft and Fraud*
- National Credit Union Administration (NCUA)
 - *How to Avoid Becoming a Victim of Identity Theft*
 - *You Can Fight Identity Theft (low resolution)*
 - *You Can Fight Identity Theft (high resolution for printing)*
- Social Security Administration
 - *Identity Theft and Your Social Security Number*
- Boston Federal Reserve Bank
 - *Identity Theft*