

What is Identity Theft?



Identity theft is using another person's identity for economic gain. Thieves tend to use your identity in one of two ways:

1. Use existing accounts to make purchases, pay for services or withdraw money
2. Open new accounts or service agreements with stolen information

How Does Identity Theft Happen?

- **Opportunistic**
e.g., stolen or lost wallets or purses, misappropriated credit or debit cards, re-approved credit applications that you've discarded
- **Intentional schemes**
e.g., asking for personal information in emails, calls or letters (called **phishing**), pretending to be you to use your benefits, applying for loans in your name

Warning Signs of Identity Theft

- ATM or bank withdrawals you didn't make
- Credit card charges you don't recognize
- Bills from medical offices you haven't visited
- Mail you're expecting that doesn't arrive
- Calls from debt collectors
- Notices from the IRS about unreported income or multiple tax returns

Protect Your Identity

- Don't share personal or account information on social media or emails
- Shred documents others could steal
- Check your credit reports routinely
- Report any suspicious financial transactions immediately to limit losses

What to Do If Your Identity Is Stolen

- Don't be embarrassed—act!
- Call your bank and credit card issuers immediately so they can close your accounts
- Put a fraud alert on your credit reports to prevent opening of new accounts
- File reports with police and Federal Trade Commission
- Follow up with the IRS, Social Security Administration, and the Centers for Medicare & Medicaid Service for theft of benefits
- Keep a record of who you contacted and when

