

Identity Theft

Workshop Goals



Copyright 2025 EverFi, Inc.

In this workshop, you will...

- 1 Learn how to identify the signs of identity theft and fraud.
- 2 Examine different types of identity theft and fraud.
- 3 Identify strategies to protect yourself from identity theft and fraud.
- 4 Learn how to protect your data using safe habits.

Sensitivity: Internal

How Much Do You Know About Identity Theft?



Poll Question:

True or False?

1. There is a victim of identity theft every 2 seconds.
2. You are more likely to have your identity stolen than have your car stolen or home burglarized.

Source: money.cnn.com

Copyright 2025 EverFi, Inc.

Sensitivity: Internal

Identity Theft and Identity Fraud

Identity theft and **identity fraud** are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way.

Identity fraud

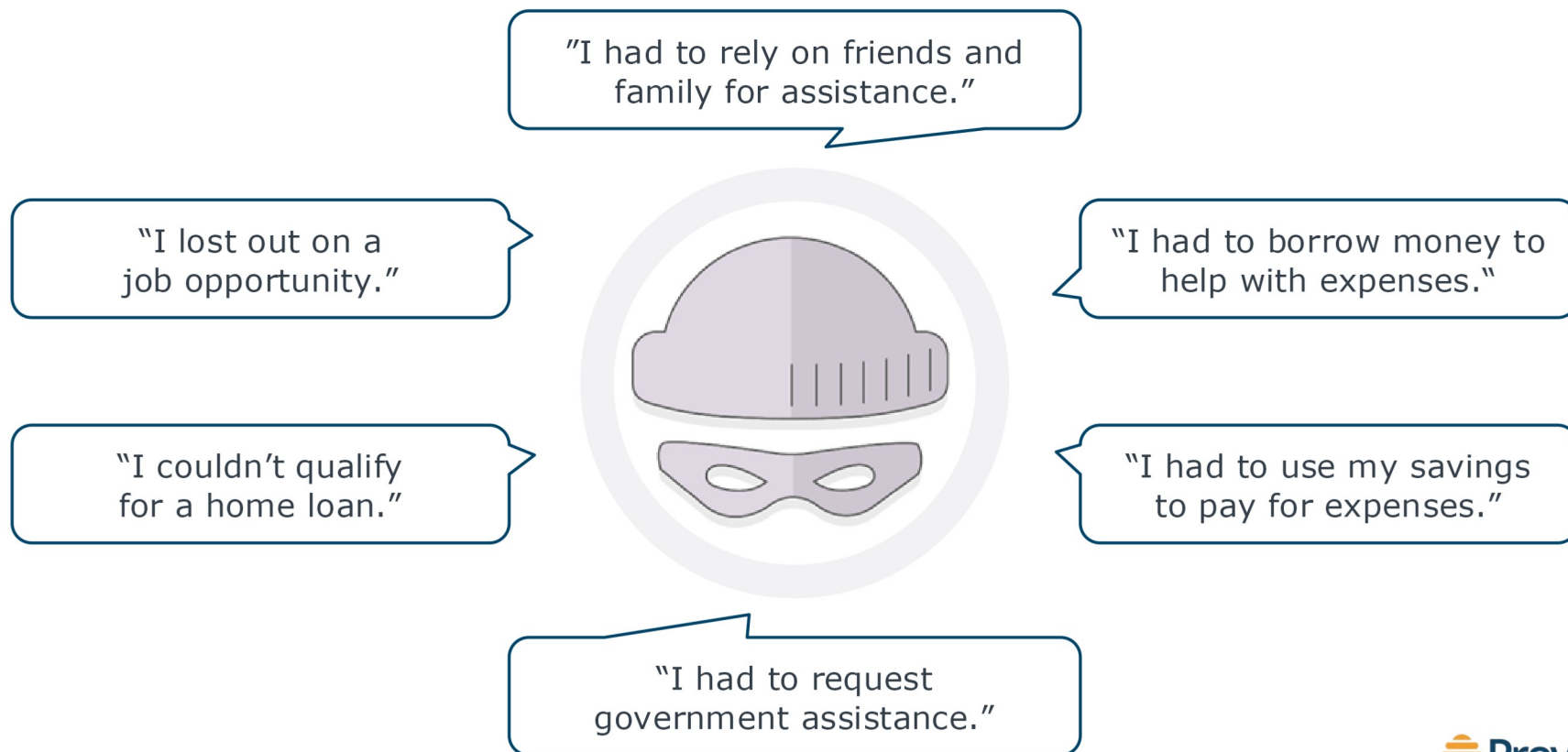
occurs when someone's personal information is used to access money.



Identity theft is when personal information is accessed, even if it isn't used for financial gain.

What Are the Effects of Identity Theft?

In a survey by ID Theft Center, victims said:



How Do Identity Thieves Use Your Identity?

- Make transactions
- Open new accounts
- Commit fraud
- Commit cybercrimes
- Get prescriptions
- Receive medical treatment



What is Personally Identifiable Information (PII)?



Biographical data:



Biographical data



Medical data



Biometric data



Financial data



All this data forms the basis of Personally Identifiable Information (PII). PII can be a piece of data or a collection of data that is unique to you and can be used to trace who you are and other personal facts about you.

What Can Be Used to Steal Your Identity?

- Social Security Number
- Name
- Birth date
- Address
- Driver's license
- Passport
- Marriage/divorce records
- Insurance cards
- Credit/debit cards
- Personal checks
- Email addresses

Copyright 2025 EverFi, Inc.

Sensitivity: Internal



Methods Used by Identity Thieves

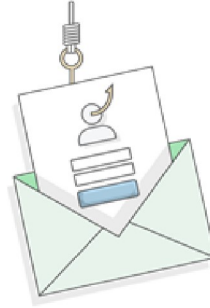
Theft



Dumpster Diving



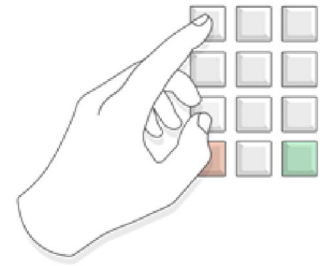
Shoulder Surfing



Mail Fraud



Skimming



Common Scams

Phishing Scams

Telephone Scams

Elder Fraud Scams



Common Scams

Phishing Email

From: National Bank <johnsmith@natonalbank.com>
To: janesmith@gmail.com
Subject: Account Freeze

Dear Customer,

2. Generic Greeting

You are receiving this email because your account has been compromised. If you do nothing your money will be gone. Please sign in using the link below or else your account and all its money will be terminated within 36 hours.

Confirm your identity here:

www.natonalbank.com/login

**4. Fake login page:
missing "i" in National Bank**

**3. Unprofessional
language**

**1. Missing "i" in
National Bank**



Phishing Email Activity

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 your account will be permanently deleted.

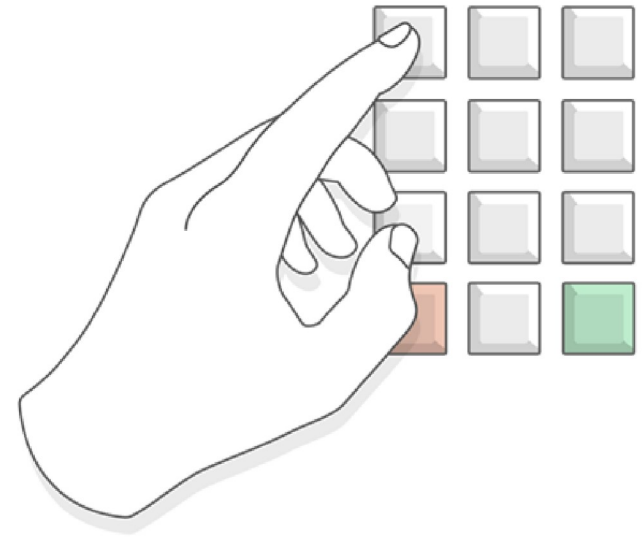
Best,
Yahoo Team

Common Scams

Phone Scams

“

Hello, Mrs. James! You are the lucky winner of the Million Dollar Lottery. Congratulations! All you need to do is verify your identity with your Social Security number and provide us with details of your bank account where we can wire you the money. I'm not supposed to tell you this, but if you act now, we should be able to waive all the taxes on the amount. I have all the paperwork with me right here. Let's start with your Social Security number..."



Phone Scams Activity



"Hi, I'm friends with your nephew. He's in trouble with the law and needs your help. He got arrested last night and is now in jail. He needs bail money before he can be released. It's a long story, but he asked me to call you instead of his parents because he is embarrassed about what happened to him. He needs you to wire money in the next hour from Western Union. It's important that you send this money right away."

Common Scams

Elder Fraud Scam

At 87, Mr. Ali lives alone in his house. His wife passed away 10 years ago and his children live in a different state. Recently, he met a young man called Sameer, who said he was Mr. Ali's long-lost nephew.

Sameer quickly moved into Mr. Ali's house and helped with his daily chores. Mr. Ali was so grateful that he agreed to give Sameer power of attorney so that he could manage the household finances.



Elder Fraud Scam Activity

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.

Special Cases of Identity Theft



Child Identity Theft

Children's personal information may be used by thieves to open accounts, apply for and use credit cards, apply for social service benefits, and so on.



Medical Identity Theft

A thief can use your medical identity to access health care, get prescription medication, or claim insurance benefits.



Tax Identity Theft

Once thieves have access to your Social Security number and name, they may file a tax return using your identity so that they receive a large tax return.

Red Flags of Identity Theft



Denials

- Denial of credit card application or services
- Denial of services (utility, rent, mortgage, etc.)



Unusual Activity

- Unusual charges on credit card or financial account
- Unusual changes in credit report and credit scores
- Unusual calls from debtors or collection agencies for debts you do not owe
- Unusual bills for services or products that you have not used
- Unusual increases in insurance or interest rates



IRS Reports

- IRS reports indicating that more than one person has filed a tax return using your SSN
- IRS reports indicating wages received from unknown sources



Medical

- Incorrect medical history information
- Incorrect medical bills



Lost Items

- Lost mail
- Lost bills

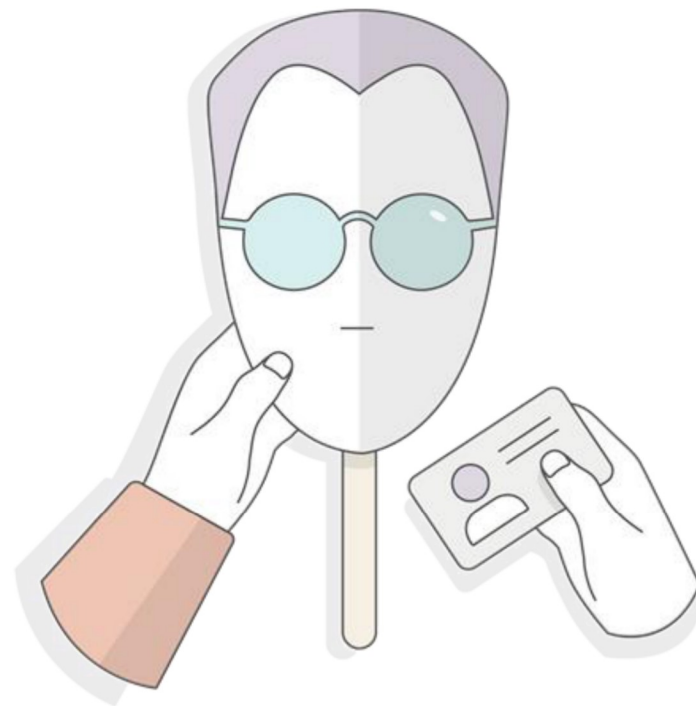
Protecting against Identity Theft: Dos and Don'ts

Dos

- Do monitor your accounts, credit reports, and credit score.
- Do monitor your financial statements.
- Do practice online safety.
- Do secure important documents.
- Do be aware of your surroundings.

Don'ts

- Don't use public Wi-Fi to access sensitive information.
- Don't click unknown links.
- Don't open suspicious attachments.



Ways to Protect Yourself Against Identity Theft

Credit monitoring services

Identity monitoring services

Credit or security freezes

Fraud alerts



How the Law Protects You

Identity Theft and Assumption Deterrence Act of 1998

This Act states that identity theft is a federal crime that can carry a punishment of up to 15 years' imprisonment.

Gramm-Leach-Bliley Act of 1999

This Act requires financial institutions to protect your data and notify you about how they use your information.

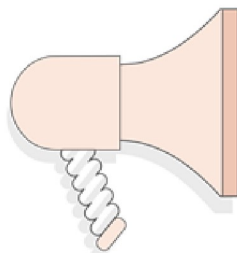


Steps to Take after Identity Theft



1

Collect information and
review accounts



2

Report to FTC, fraud
departments, and law
enforcement



3

Repair damage

Summary

In this workshop, you...



Copyright 2025 EverFi, Inc.

- 1 Learned how to identify the signs of identity theft and fraud.
- 2 Examined different types of identity theft and fraud.
- 3 Identified strategies to protect yourself from identity theft and fraud.
- 4 Learned strategies to protect your data using safe habits.