



LifeSmarts

Learn it. Live it.

Key Points

YOUR IDENTITY IS A VALUABLE TARGET

Criminals steal personal data to open accounts, drain funds, or commit crimes in your name.

FRAUD COMES IN MANY FORMS

From phishing emails to QR code scams, modern fraud is diverse and constantly evolving.

TECHNOLOGY MAKES FRAUD EASIER & FASTER

Scammers use automation, spoofing tools, and stolen data to reach thousands of victims in seconds.

SCAMS OFTEN START WITH TRUST

Fraudsters pose as banks, family members, or government officials to trick you into acting fast.

Core Concepts

ACCOUNT TAKEOVER

When a criminal gains access to your existing accounts, they can change passwords, lock you out, and steal funds.

SYNTHETIC IDENTITY THEFT

Combining real and fake information to create a new identity makes it harder to detect, and harder to stop.

CREDENTIAL STUFFING

If you reuse passwords, one stolen login could unlock multiple accounts.

PHISHING VS. SMISHING

Phishing comes through email, while smishing arrives by text... both trick you into giving up personal info.

QR CODE SCAMS

Fraudsters may post fake codes in public places to redirect you to malicious websites.

SIM SWAP FRAUD

A scammer convinces your phone carrier to switch your number to a new SIM, gaining control of texts and calls.

IMPOSTER SCAMS

You get a message from someone pretending to be your grandparent, your boss, or the IRS and they create panic to get money.

StudySmart Guide - StudySmart Guide - StudySmart Guide - StudySmart Guide

The New Face of Fraud

Additional Resources

Federal Trade Commission – Identity Theft

Official FTC site for reporting identity theft and getting a personalized recovery plan

<https://bit.ly/4lozoWj>

Consumer Financial Protection Bureau – How to Spot Fraud

Guidance on recognizing common scams and taking action to protect yourself

<https://bit.ly/3JaFDzk>

YouTube - New Scams to Watch Out for 2025

Scammers keep adapting... see what they're up to now

<http://bit.ly/4IEkJXb>

YouTube - Cybercrime: Hacking Goes Way Beyond Simple Identity Theft

Security expert Marc Goodman explains how modern cybercrime has evolved

<https://bit.ly/41wILNr>

Listen to the Podcast



Explore and Explain

1. How do criminals steal personal information to commit identity theft?
2. What warning signs might indicate that your identity has been stolen or misused?
3. How can protecting your personal information online and offline help prevent fraud?
4. What steps should you take if you become a victim of identity theft?

Fraud and identity theft can cause serious financial and legal problems, but knowing how to protect yourself, and how to respond, can limit the damage.

Fraud & Identity Theft

Acronyms

2FA

Two-Factor Authentication

FCRA

Fair Credit Reporting Act

KBA

Knowledge-Based Authentication

PIN

Personal Identification Number

SSN

Social Security Number



LifeSmarts

Learn it. Live it.

Vocabulary

ACCOUNT TAKEOVER

When someone gains control of your existing account (like email or banking) to steal money or data

CREDENTIAL STUFFING

Using stolen usernames and passwords from one site to try and access accounts on other sites

IDENTITY MONITORING

A service that checks if your personal data is being misused or sold online

IMPOSTER SCAM

When someone pretends to be a trusted person or company to trick you into sending money or info

PASSKEY

A modern login method that replaces passwords with encrypted credentials tied to your device or biometrics—safer and resistant to phishing

QR CODE SCAM

A fake QR code placed in public to trick people into visiting malicious websites or giving up information

SIM SWAP SCAM

When a scammer tricks your phone provider into switching your number to a new SIM card they control

SYNTHETIC IDENTITY THEFT

Using a mix of real and fake information to create a new, false identity for financial gain

TOKENIZATION

A security process that replaces sensitive info (like credit card numbers) with a useless placeholder

Sponsored by:
experian™