Cybersecurity & Avoiding Identity Theft

Dark Web, Social Engineering, & Scams

Tobi West, PhD
March 2025

bit.ly/CSUF-OLLI-March2025

Tobi West

PhD

Cyber Defense, Dakota State University

Cybersecurity Professor

Technology Department Chair, Coastline College

Cyber Center Director

National Center of Academic Excellence in Cybersecurity

www.tobiwest.com

Topics

01 **Intro**
Key threats

02 **Identity Theft**
Definition and types

03 **Impact**
Real-world consequences

04 **Protecting Yourself**
Best practices

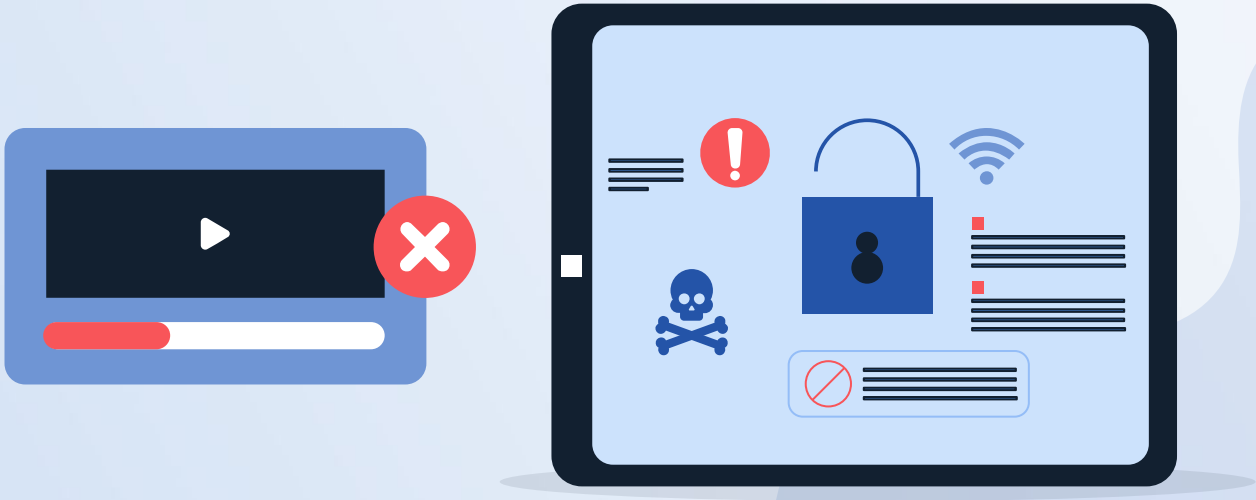
05 **Responding**
Immediate actions

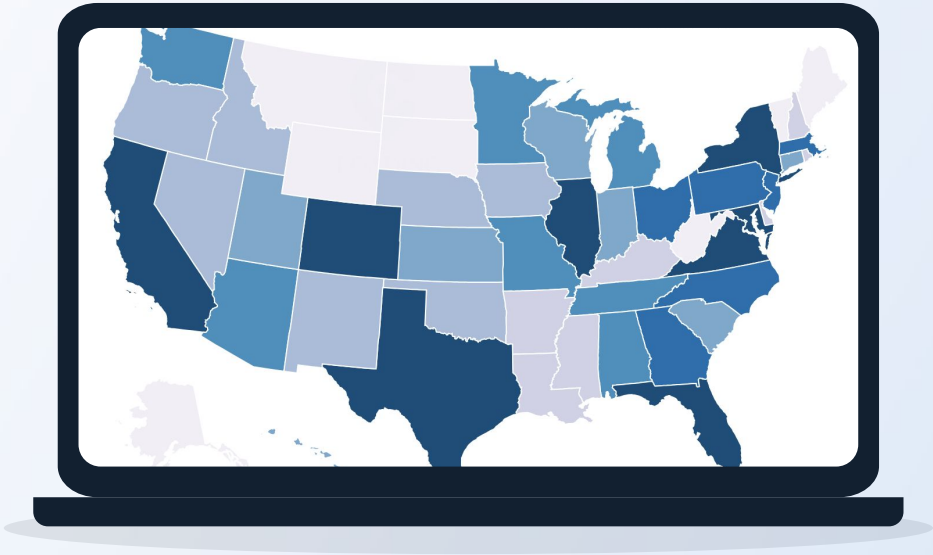
06 **Resources**
For further learning

Access the slides

01 Introduction

Cybersecurity & Identity Theft





457,398

Cybersecurity job openings
in the United States

www.cyberseek.org

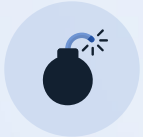
Cybersecurity

The practices, technologies, and processes designed to protect digital systems, networks, and sensitive information from cyber threats.

Importance of Cybersecurity

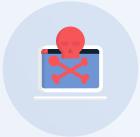
Cyberattacks

Threats and attacks are continually on the rise



Data

Personal and financial data continues to increase in value



Impact

Individuals, businesses, and governments

Zero Day on Netflix

Motives for Cyberattacks

Political

Protest

Angry / Interfere with elections

Financial

Money

Small scale to large scale

Status

Fame

On the dark web or public acknowledgement

Espionage

Sabotage

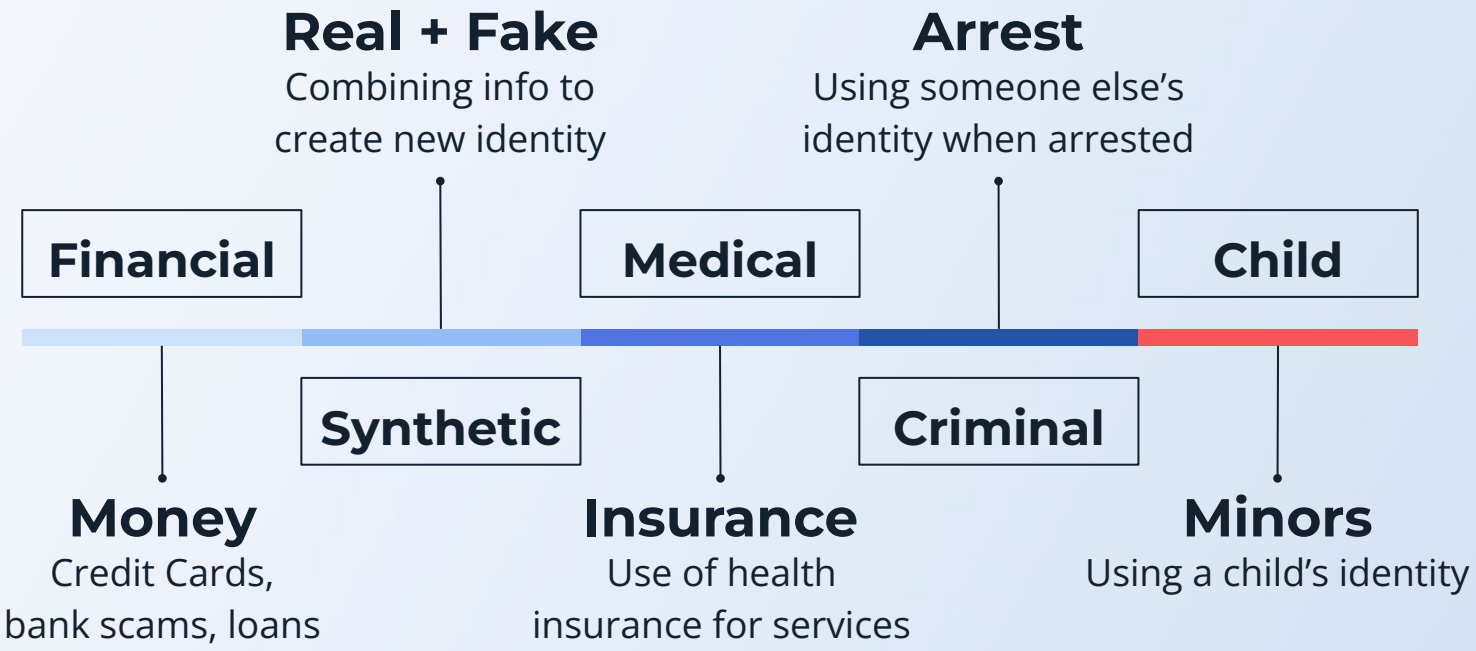
Trade secrets Technical schematics

ID Theft

Occurs when someone unlawfully uses another person's personal information for fraud or deception.

(e.g., name, Social Security number, credit card information)

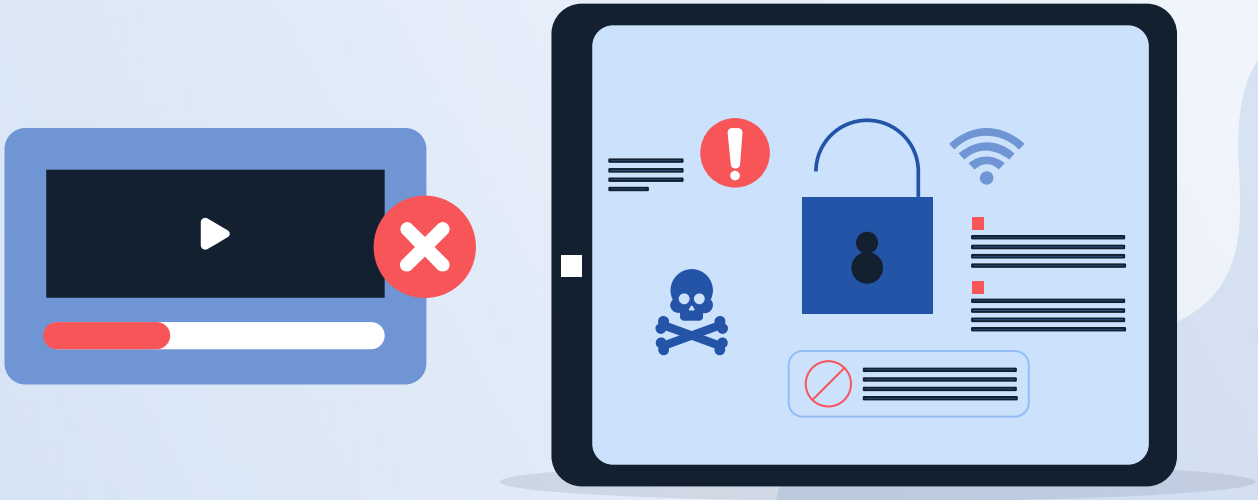
Types of Identity Theft



www.identitytheft.gov

02 Identity Theft

Key terms



2.6M Cases
$12.5B in fraud loss
1.1M Cases
FTC IdentityTheft.gov

Understanding ID Theft

Phishing

“Friendly” email to steal login credentials

Smishing

Fake text and phone calls to trick victims

Data Breaches

Exposure of records (e.g., Equifax, Target)

Social Engineering

Manipulating people to get sensitive info

Skimming

Devices placed on ATMs and gas pumps to get credit card info

Weak Passwords

Reusing passwords on multiple sites makes them vulnerable

Dark Web

Common web browser

No login required

Common web browser

Login required

Special web browser

Login/no login

Seller

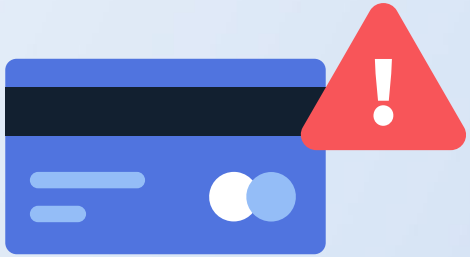
Criminals sell personal data, credit card numbers, and Social Security numbers

Buyer

Uses the stolen data for fraud, blackmail, and identity theft

Examples

$5 for credit card number
$250 for medical record ($1-$1,000)



03 Impact

Consequences of identity theft

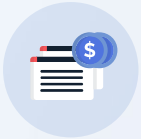
Personal Consequences

Financial Loss

Unauthorized transactions, loans, & debts in your name

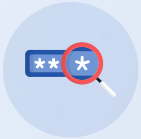
Legal Issues

May have to prove your innocence



Credit Damage

Lower credit score, difficulty getting loans



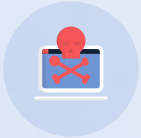
Stress

Emotional & Psychological
Victims often feel isolated, stressed, and anxious

Business & Organizational

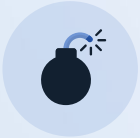
Legal & Compliance Issues

Companies face lawsuits if they fail to protect customer data



Reputation Damage

Loss of customer trust after a data breach



Operational Disruptions

Cyberattacks can shut down business operations

04 Protecting Yourself

Against identity theft

Best Practices for Individuals

MFA

Strong passwords & multi-factor authentication

Stop...Think

Never click on suspicious links in email or texts

Lock Screen

Secure personal devices

Updates

Software, operating systems, & anti-virus software

Monitor

Check financial accounts, credit reports, & use monitoring service

Freeze Credit

When necessary to prevent accounts from being opened

Cyber Scams

Honey Traps
Romance scams
Online games
Social Media
Spoofing
Information gathering
Email
Online
Web
Games
Sites
Phishing
Spoofing
Urgency, typos
Shopping
Be aware of
legitimate sites
Lock
Fake sites
Look for the lock

Identity Theft Protection

	lost wallet protection	24x7 support	reimbursement
	Credit score monitoring	Court records & bookings	Banks
	Dark Web monitoring	US Postal Service (redirect)	Sex offenders
	Social media monitoring	SSN (addresses)	Driver's license

Aura | Lifelock | Identity Guard

10 Day Security Fix

REVIEW / EDIT / DEL	REMOVAL & OPT OUT	MINDSET
Make 3 lists: devices, accounts, people	Data Brokers	Secure & Skeptical
Reused passwords: change **Old accounts:** edit & delete **Previous posts:** review & delete **Social media:** privacy setting	**Search your name** **Search your address** **This can take time**	**Freeze/Monitor Credit** **VPN** **Temporary CC number** **Keep devices & apps updated**

!@#$ PASSWORDS %^&*

Longer passwords are better. Avoid top 100.

Try Bitwarden. It's free!

- Use consumer reports to find pw manager
- Share passwords across devices
- Create strong passwords
- Audit passwords

Passwords can still end up on the darkweb!

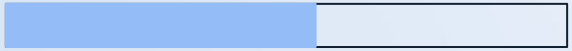
Use multi-factor authentication.

www.bitwarden.com

Best Practices for Business

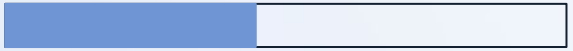
Awareness Training

Cybersecurity training for employees



Strong Security Policies

Using encryption and secure password policies

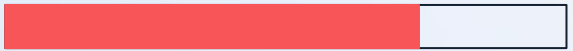


Security Audits

Identify and mitigate vulnerabilities

Data Protection

Encrypt sensitive information & secure servers



05 Responding

To Identity Theft

Immediate Actions

Bank & Cards

Contact

Call to report fraudulent transactions

Credit Bureau

Alert

Place a fraud alert or freeze your credit

Police & FTC

Report

Contact law enforcement & IdentityTheft.gov

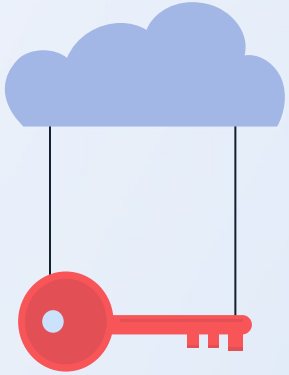
Bank & Credit

Monitor

Watch for further unauthorized activity

Dispute

Fraudulent charges and accounts



Prevent

Avoid future incidents

Repair

Work to recover your credit score

06 Resources

Takeaways and further learning

Key Takeaways

- Use strong, unique passwords & enable multi-factor authentication (MFA)
- Monitor your credit reports and financial statements regularly
- Freeze your credit if you're not applying for loans or credit
- Be cautious of phishing scams and social engineering tactics
- Avoid sharing personal information over email, text, or phone calls

Government & Law Enforcement Resources

- **IdentityTheft.gov (FTC)**
  - Official Federal Trade Commission (FTC) site for reporting identity theft.
  - Provides step-by-step recovery plans.
- **USA.gov - Identity Theft**
  - Government guide on preventing and responding to identity theft.
- **Federal Trade Commission (FTC) - Consumer Information**
  - Information on identity theft prevention and fraud alerts.
- **Social Security Administration (SSA) - Identity Theft Help**
  - Steps to take if your Social Security number is stolen.
- **FBI Cyber Crime Division (Internet Crime Complaint Center - IC3)**
  - Report cybercrime and identity theft-related fraud.
- **US Department of Justice (DOJ) - Identity Theft**
  - Legal guidance and identity theft protection tips.

Credit Monitoring & Fraud Alerts

- AnnualCreditReport.com
  - The only **official** site to get a **free credit report** from Equifax, Experian, and TransUnion once a year.
- **Credit Bureaus (for Fraud Alerts & Freezes):**
  - **Equifax - (1-888-298-0045)**
  - **Experian - (1-888-397-3742)**
  - **TransUnion - (1-800-680-7289)**

Non-Profit & Consumer Protection

- **Identity Theft Resource Center (ITRC)**
  - Free victim assistance and education.
- **Better Business Bureau (BBB) Scam Tracker**
  - Report identity theft scams.
- **Privacy Rights Clearinghouse**
  - Information on privacy protection and identity theft prevention.
- **National Cybersecurity Alliance (NCSA)**
  - Cybersecurity tips and identity theft prevention resources.

Dark Web & Data Breach Monitoring

- **Have I Been Pwned**
  - Check if your email or personal data has been leaked in a data breach.
- **Dark Web Monitoring Services:**
  - **Experian Dark Web Scan** (Experian)
  - **Norton LifeLock Dark Web Monitoring** (Norton)
  - **Identity Guard** (Identity Guard)

ID Theft Protection & Recovery Services

- **LifeLock by Norton**
  - Paid identity theft monitoring and recovery services.
- **ID Watchdog**
  - Identity theft resolution and credit monitoring.

Cybersecurity is everyone's responsibility.

Stay aware, stay secure!

Thanks

Tobi West, PhD
Technology Department Chair
Cyber Center Director

twest20@coastline.edu
www.coastline.edu/cybercenter
www.cybertechgirls.org