CSNP
CYBERSECURITY NON-PROFIT

Identity Protection Guide for Women

Your comprehensive resource for safeguarding your personal information and digital identity in today's connected world.

WHY IT MATTERS

The Importance of Identity Protection

Identity theft affects millions annually, with women particularly vulnerable to targeted attacks including stalking, harassment, and financial fraud. Your personal information is a valuable asset that requires active protection.

The digital age has made our lives more convenient, but it's also created new vulnerabilities. Understanding these risks empowers you to take control of your digital footprint and protect yourself.

33%

Identity Theft

Percentage of women who experience identity theft in their lifetime

15M

Annual Victims

Americans affected by identity fraud each year

Understanding Personal Information Exposure

Your personal information exists in more places than you realize. Data brokers collect and sell details about your life, while public records databases make information easily accessible to anyone with internet access.

Public Records

Property records, voter registration, and court documents can reveal your address, age, and family connections. Consider opting out of public databases when possible.

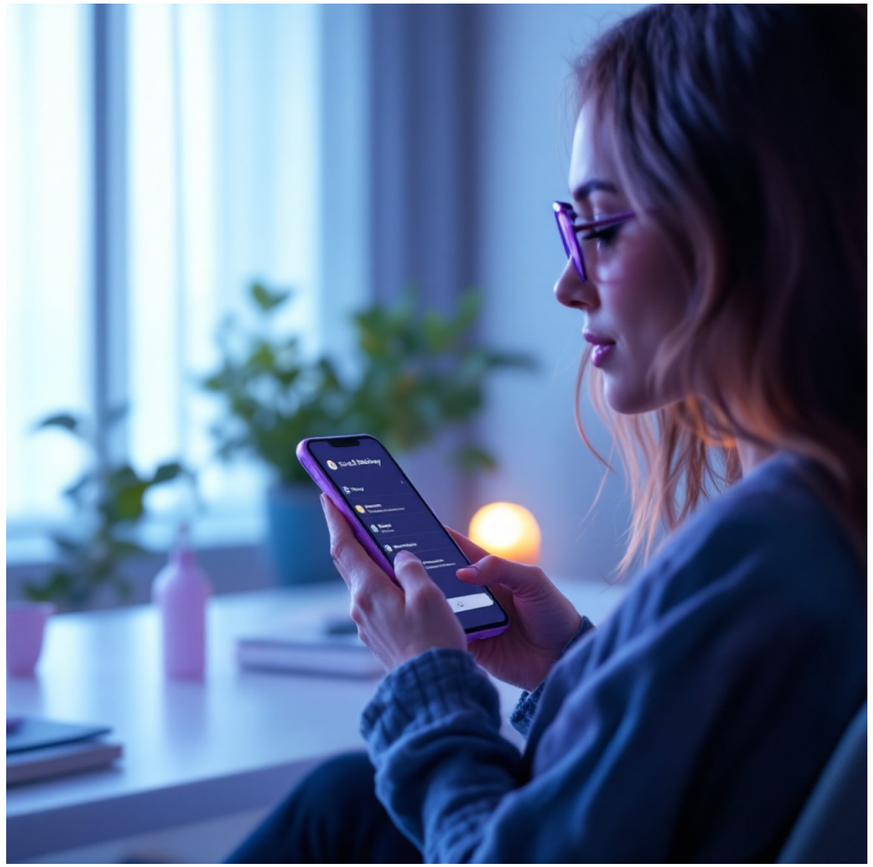
Data Brokers

Companies compile and sell your information to marketers, employers, and others. Request removal from major data broker sites regularly.

Online Accounts

Every account you create leaves a trail. Use unique passwords and review privacy settings frequently to limit exposure.

Social Media: Your Digital Storefront



Social media oversharing creates a detailed map of your life for potential bad actors. Location tags, check-ins, and personal details shared innocently can be weaponized.

Smart Sharing Guidelines

- Avoid posting real-time locations or vacation plans
- Review and limit who can see your posts
- Remove metadata from photos before sharing
- Think twice before sharing children's names or schools
- Disable location services for social media apps

Protecting Your Physical Address

01

Use a PO Box or Private Mailbox

For online purchases, subscriptions, and non-essential mail to keep your home address private.

02

Opt Out of Data Broker Sites

Submit removal requests to Whitepages, Spokeo, BeenVerified, and other people-search websites.

03

Register with State Programs

Many states offer address confidentiality programs for domestic violence survivors and others at risk.

04

Be Cautious with Deliveries

Use pickup locations or delivery lockers when available, especially for high-value items.

PRIVACY FIRST

Phone Number Privacy Strategies

Why It Matters

Your phone number is a gateway to your identity. It's used for account recovery, two-factor authentication, and can reveal your location and personal connections.

Google Voice

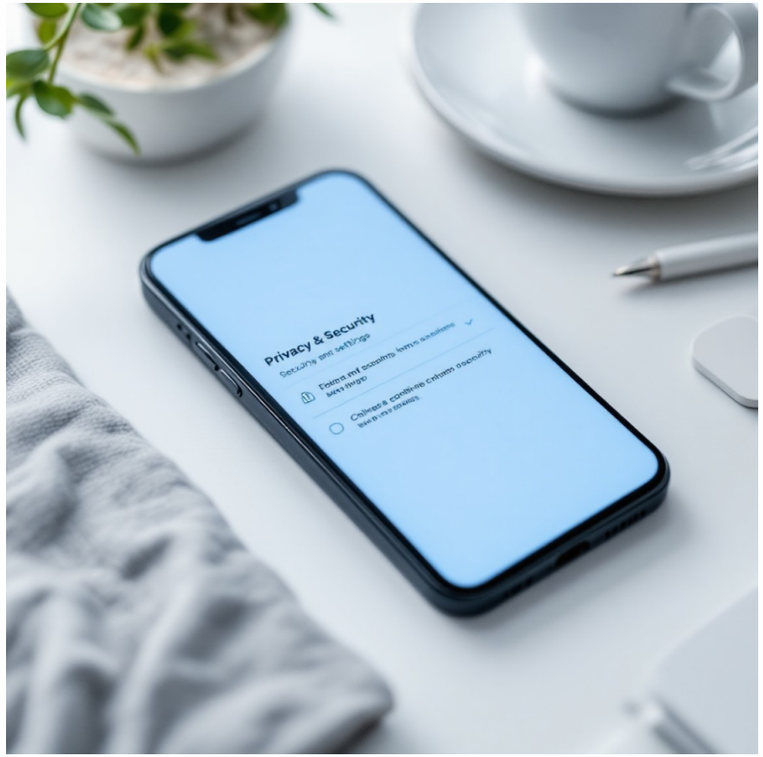
Create a free secondary number for online accounts and untrusted services.

Carrier Features

Enable spam blocking and unknown caller screening through your mobile provider.

Best Practices

- Never share your primary number on public forms
- Use separate numbers for work and personal life
- Enable caller ID blocking when making calls
- Remove your number from marketing lists via donotcall.gov
- Consider using authentication apps instead of SMS for 2FA



Credit Monitoring & Financial Security

Freeze Your Credit

Place a security freeze with all three bureaus (Equifax, Experian, TransUnion) to prevent unauthorized accounts. It's free and highly effective.

Set Up Monitoring

Use free services like Credit Karma or your credit card's monitoring tools to receive alerts about new accounts or inquiries.

Review Regularly

Check your credit reports annually through AnnualCreditReport.com for suspicious activity or errors.

Secure Accounts

Enable two-factor authentication on financial accounts and use strong, unique passwords for each institution.

Document Security Essentials

Physical and digital documents containing personal information require careful handling to prevent identity theft and fraud.

Secure Storage

Keep sensitive documents in a locked safe or filing cabinet. Store digital copies in encrypted, password-protected folders.

Proper Disposal

Shred documents containing Social Security numbers, account numbers, or other sensitive data before discarding.

Digital Backups

Use encrypted cloud storage or external drives for important documents. Never store sensitive files on unprotected devices.

Documents to Protect

- Social Security cards
- Birth certificates
- Passports
- Tax returns
- Bank statements
- Medical records
- Insurance policies

If Your Identity Is Compromised

Quick action is essential if you suspect identity theft. Follow these steps immediately to minimize damage and begin recovery.

1

Contact Financial Institutions

Alert your bank and credit card companies. Close compromised accounts and open new ones with enhanced security.

2

File Reports

Report to IdentityTheft.gov and file a police report. These documents are crucial for disputing fraudulent charges.

3

Place Fraud Alerts

Contact one credit bureau to place a fraud alert on your credit reports. They'll notify the other two bureaus automatically.

4

Document Everything

Keep detailed records of all communications, including dates, names, and case numbers for future reference.

5

Monitor Ongoing

Continue monitoring accounts and credit reports closely for at least a year after the incident.

About Cybersecurity Non-Profit (CSNP)

> *"Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."*

Our Programs

Business & Non-Profit Security

Family Cybersecurity

Kids Safety

Senior Digital Safety

Women's Security

Parents & Educators

Everything we offer is completely free. Visit us online to access resources, workshops, and community support.

Visit csnp.org

Browse Resources