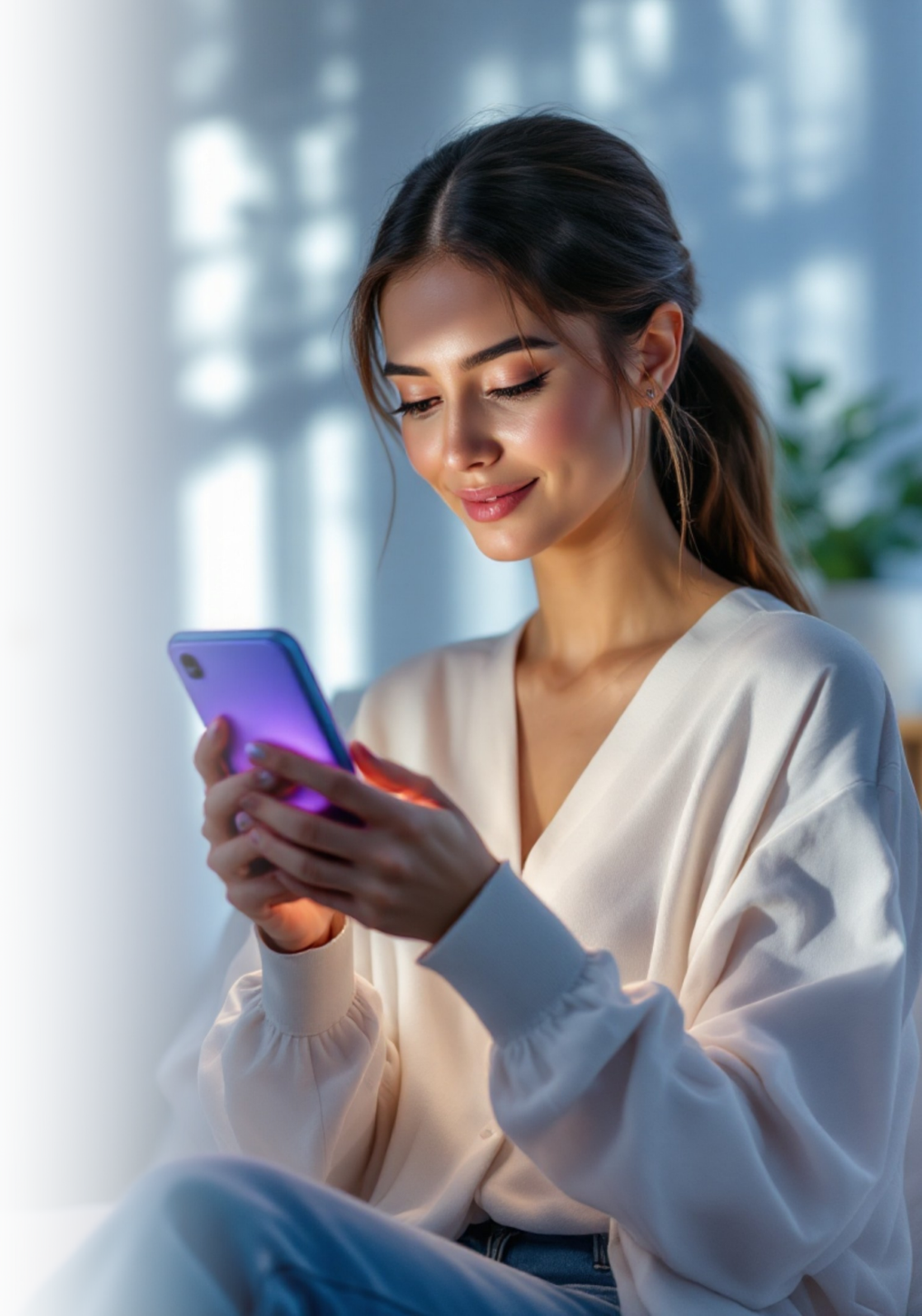
CSNP
CYBERSECURITY NON-PROFIT

Digital Stalking Prevention Guide

Protecting your digital privacy and safety in an increasingly connected world. A comprehensive guide from the Cybersecurity Non-Profit.



UNDERSTANDING THE THREAT

What is Digital Stalking?

Digital stalking is the use of technology to monitor, harass, or track someone without their consent. It can include tracking your location, accessing your accounts, monitoring your communications, or gathering information about you online.

This behavior is a form of abuse that can make you feel unsafe, violated, and constantly watched. Understanding the tactics used is the first step toward protection.

You are not alone. Digital stalking affects millions of people. Taking steps to protect yourself is not paranoia—it's empowerment.

Recognize the Warning Signs

Unexplained Knowledge

Someone knows details about your activities, locations, or conversations they shouldn't have access to.

Device Behavior

Your phone or computer acts strangely—unexpected battery drain, unusual data usage, or apps you didn't install.

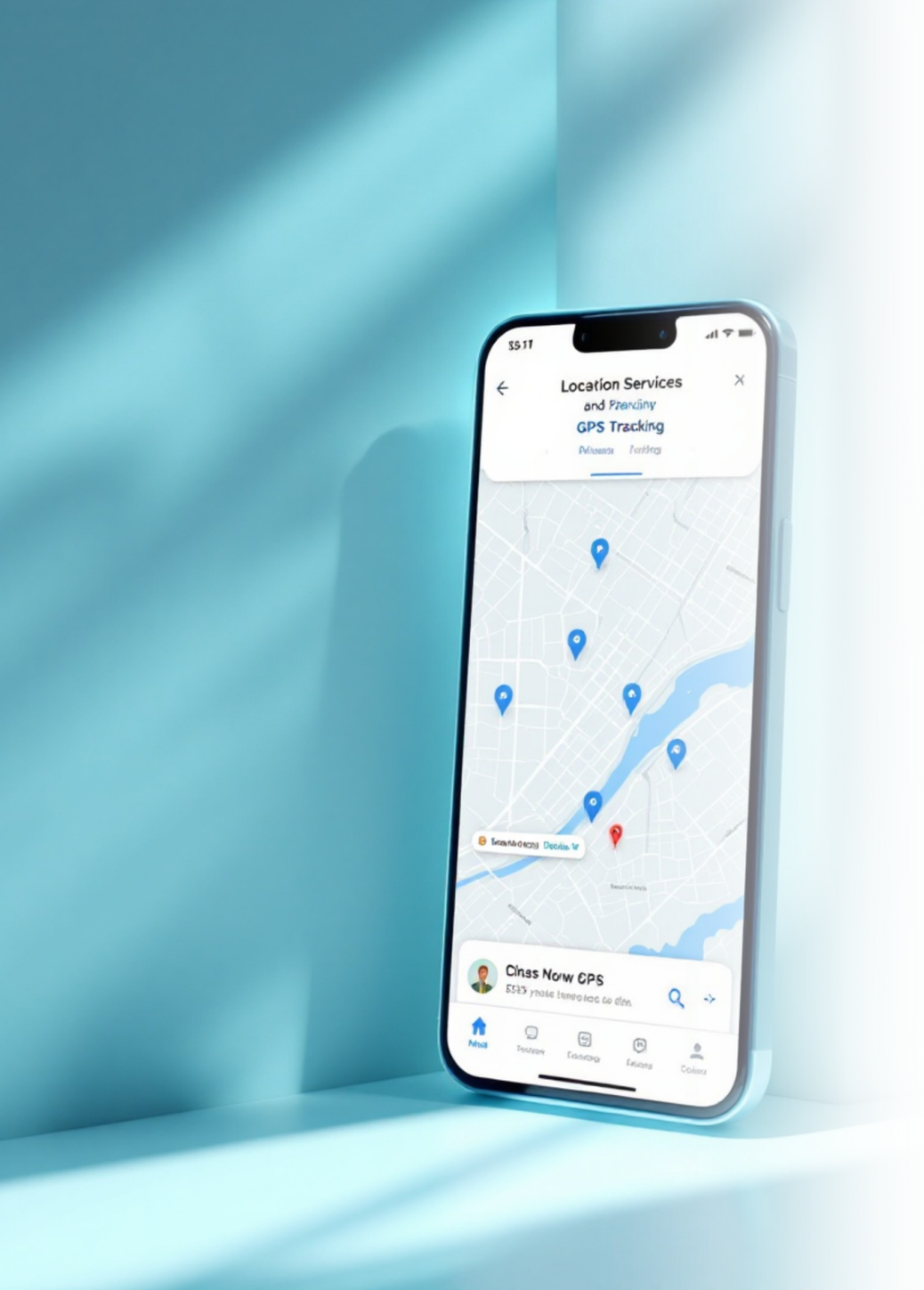
Account Access

You notice login attempts, password changes, or activity you didn't authorize on your accounts.

Persistent Contact

Someone consistently appears in places you visit or contacts you across multiple platforms after being blocked.

Trust your instincts. If something feels wrong, it's worth investigating further.



Location Tracking Threats

Find My Phone Features

Check if someone has access to location-sharing services like Find My iPhone or Google's Find My Device.

Social Media Geotagging

Disable location tagging on photos and posts. Past posts may reveal your home or workplace.

Vehicle GPS Trackers

Physical tracking devices can be hidden in your car. Check under bumpers, wheel wells, and inside the vehicle.

SOCIAL MEDIA SAFETY

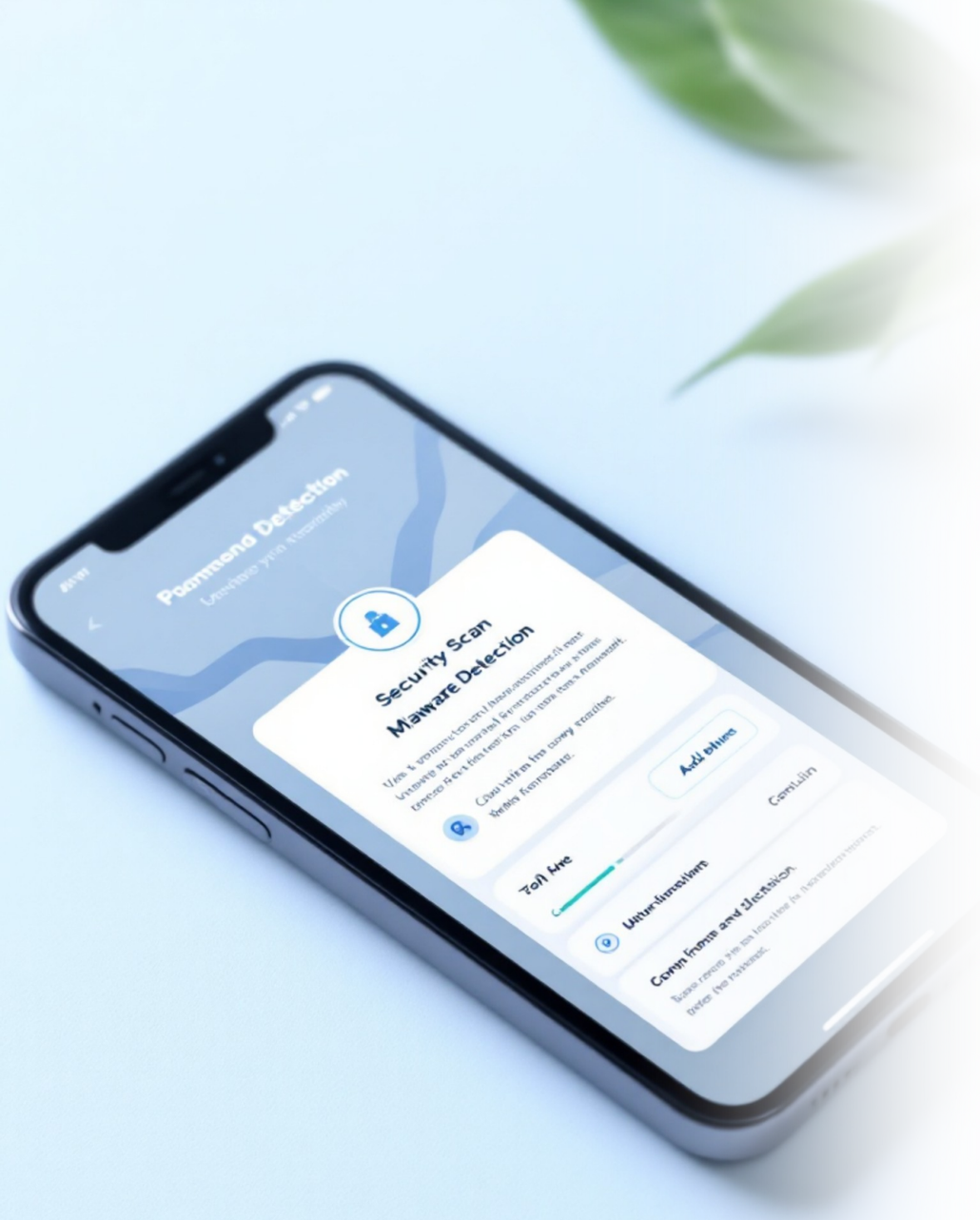
Protecting Your Social Media Presence

Immediate Actions

- Review and restrict your privacy settings on all platforms
- Remove location data from photos before posting
- Be cautious about sharing your schedule or routines
- Review your follower and friend lists regularly
- Disable tagging without your approval

Advanced Protection

- Create separate accounts for public and private sharing
- Use different usernames across platforms
- Avoid posting real-time updates about your location
- Block and report suspicious accounts immediately
- Consider making accounts private or temporarily deactivating them



Detecting Spyware and Monitoring Apps

01

Check Installed Apps

Review all apps on your device. Look for unfamiliar names or apps disguised as system services. Common stalkerware includes mSpy, FlexiSPY, and Spyic.

02

Monitor Battery and Data Usage

Spyware runs constantly in the background. Check your settings for apps using excessive battery or data compared to their normal function.

03

Look for Jailbreaking or Rooting

Check if your phone has been jailbroken (iPhone) or rooted (Android). This allows hidden apps to operate with expanded permissions.

04

Use Detection Tools

Install reputable anti-spyware apps like Certo Mobile Security or Kaspersky. They can identify monitoring software on your device.

Comprehensive Device Security Check

Secure Your Devices

- Change all passwords and PINs immediately
- Enable two-factor authentication on everything
- Update to the latest operating system
- Factory reset if you suspect compromise

Review Permissions

- Audit app permissions for location, camera, and microphone
- Revoke unnecessary access
- Check connected devices and authorized apps
- Review recent account activity

Physical Security

- Keep devices password-protected at all times
- Never share your unlock code
- Disable automatic backups to shared accounts
- Use biometric locks when available

Securing Your Online Accounts

1

Create New Email

Set up a new email address that only trusted people know. Use it for important account recoveries.

2

Change All Passwords

Use unique, strong passwords for every account. Consider a password manager like Bitwarden or 1Password.

3

Enable Two-Factor Authentication

Add an extra layer of protection. Use an authenticator app rather than SMS when possible.

4

Review Connected Apps

Remove third-party app access from your accounts. Check Google, Facebook, and Apple account permissions.

TAKING ACTION

Documentation and Evidence Collection

1

Screenshot Everything

Capture threatening messages, suspicious account activity, and any evidence of stalking. Include dates and timestamps.

2

Keep a Detailed Log

Document every incident with dates, times, locations, and descriptions. Note witnesses if applicable.

3

Preserve Digital Evidence

Save emails and messages. Back up evidence to multiple secure locations, including cloud storage with strong passwords.

4

Don't Confront

Avoid alerting the stalker that you're collecting evidence. Don't delete anything—it may be needed for legal action.

This documentation can be crucial for obtaining restraining orders or pursuing legal action.

Legal Resources and Reporting

Who to Contact

- **Local Law Enforcement**

  File a police report. Bring all documentation and evidence you've collected.

- **National Hotlines**

  National Domestic Violence Hotline: 1-800-799-7233. They can provide resources and safety planning.

- **Legal Aid Organizations**

  Many offer free assistance with restraining orders and navigating the legal system.

- **Cyber Civil Rights Initiative**

  Provides resources specifically for tech-enabled abuse and can help with reporting.

Your safety matters. Digital stalking is illegal in many jurisdictions. You have the right to seek protection and hold perpetrators accountable.

Creating Your Safety Plan

1

Immediate Safety

Identify a safe place to go if needed. Tell trusted friends or family about the situation. Keep important documents accessible.

2

Digital Protection

Secure all devices and accounts. Consider getting a new phone number. Use a VPN for browsing privacy.

3

Support Network

Reach out to domestic violence organizations. Consider therapy or support groups. Share your safety plan with trusted individuals.

4

Long-term Security

Regularly update your security measures. Stay informed about new threats. Continue documenting any incidents.

Remember: Your safety is the priority. Take things one step at a time, and don't hesitate to seek professional help.

About Cybersecurity Non-Profit

"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 Our Website

csnp.org

Access Free Resources

csnp.org/resources