CSNP
CYBERSECURITY NON-PROFIT

Digital Safety Guide for Survivors

A comprehensive resource to help you recognize, address, and protect yourself from technology-enabled abuse. You deserve safety, privacy, and control over your digital life.

UNDERSTANDING TECH ABUSE

What is Technology-Enabled Abuse?

Technology-enabled abuse occurs when abusers use digital tools to monitor, control, harass, or threaten survivors. This can include tracking your location, reading your messages, controlling your accounts, or using technology to intimidate you.

Understanding these tactics is the first step toward reclaiming your digital safety and autonomy.

Recognizing Signs of Tech Control

Unusual Device Behavior

Your phone battery drains quickly, overheats, or shows apps you didn't install. Settings change without your knowledge.

Knowledge They Shouldn't Have

Someone knows details about your location, conversations, or activities that you never shared with them.

Account Access Issues

You're locked out of accounts, passwords change mysteriously, or you receive notifications about logins from unknown locations.

Constant Surveillance

Feeling watched or monitored through your devices. Receiving immediate responses about your whereabouts or actions.

DEVICE SAFETY

Is Your Device Being Monitored?

1 Check for Unfamiliar Apps

Review all installed applications. Look for apps you don't recognize, especially those with generic names or hidden icons.

2 Review Permissions

Check which apps have access to your location, camera, microphone, and messages. Revoke unnecessary permissions immediately.

3 Monitor Data Usage

Spyware often uses significant data. Check your data usage by app to identify suspicious activity.

4 Look for Device Admin Apps

Check Settings > Security > Device Administrators for apps that have administrative control over your device.

Common Spyware Detection Methods

Warning Signs

- Battery draining faster than usual
- Device running hot when idle
- Increased data usage
- Strange background noises during calls
- Unexpected shutdowns or restarts
- Browser redirects to unfamiliar sites

Important Safety Note

If you suspect spyware, don't immediately remove it if you're still in danger. Removing it may alert the abuser. Instead, use a separate, secure device to seek help and create a safety plan first.

Consider factory resetting your device only when you're in a safe location and have backed up important evidence.

COMMUNICATION

Communicating Safely

Use Encrypted Apps

Signal offers end-to-end encryption and disappearing messages. Download on a device the abuser doesn't have access to.

Use Public Devices

Access sensitive information from library computers or trusted friends' devices when possible.

Use Private Browsing

Always use incognito/private mode and clear history after each session when researching safety resources.

Remember: If your device may be monitored, avoid using it for safety planning. Reach out using a trusted device instead.

Securing Your Accounts

01

Create New Email Accounts

Open a new email account on a safe device that the abuser doesn't know about. Use it for all safety-related communications.

02

Change All Passwords

Use strong, unique passwords for each account. Consider using a password manager on your secure device.

03

Enable Two-Factor Authentication

Use authentication apps rather than SMS when possible, as phone numbers can be more easily compromised.

04

Review Account Recovery Options

Update security questions and recovery phone numbers/emails to information only you control.

05

Check Connected Devices

Review and remove unfamiliar devices from your Google, Apple, or social media accounts.

LOCATION PRIVACY

Protecting Your Location

- **Disable Location Services**

  Turn off GPS and location services for apps that don't need them. Review location permissions regularly.

- **Remove Location from Photos**

  Disable geotagging in your camera settings. Check photo metadata before sharing images online.

- **Be Careful with Check-ins**

  Avoid posting your location on social media in real-time. Consider sharing experiences after you've left.

- **Check Find My Device Settings**

  Review who has access to location sharing services like Find My iPhone or Google's Find My Device.

Documenting Evidence Safely

1

Screenshots

Take screenshots of threatening messages, unusual account activity, or evidence of monitoring. Save with dates and context.

2

Secure Storage

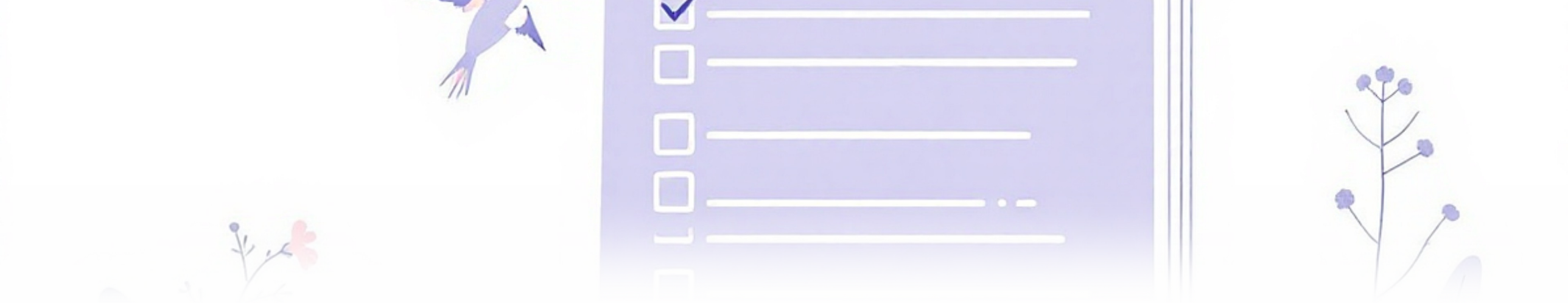
Store evidence on a device the abuser can't access, in a cloud account they don't know about, or with a trusted person.

3

Physical Copies

Print important evidence and keep it in a safe location outside your home, like with a trusted friend or attorney.

Legal Note: Documentation can be crucial for restraining orders and legal proceedings. Consult with a domestic violence advocate about the best way to preserve evidence in your situation.



SAFETY PLANNING

Creating Your Digital Safety Plan

Immediate Actions

- Get a safe device if possible
- Change passwords on a secure device
- Enable two-factor authentication
- Review all app permissions
- Check connected devices
- Disable location sharing

Ongoing Protection

- Regularly check for spyware
- Use encrypted messaging
- Maintain separate accounts
- Document incidents safely
- Stay connected with advocates
- Update your safety plan regularly

You Are Not Alone — Help is Available

National Domestic Violence Hotline

1-800-799-7233

24/7 support, safety planning, and resources. Text "START" to 88788.

National Sexual Assault Hotline

1-800-656-4673

Confidential support from trained staff members.

Tech Safety Resources

csnp.org/resources

Free guides, tools, and step-by-step instructions for digital safety.

These hotlines can connect you with local resources, help with safety planning, and provide emotional support. Your safety is the priority.

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 Online
- Senior Digital Safety
- Women's Security & Privacy
- Parents & Educators Resources

Everything we offer is completely free.

Connect With Us

Visit our website for comprehensive resources, guides, and support:

Website: csnp.org

Resources: csnp.org/resources

We're here to help you build digital safety skills and reclaim control over your technology.