



Digital Privacy & Online Protection Checklist for Survivors

SurvivorsRights.com Confidential Support Resource

After sexual abuse or assault, survivors often worry about retaliation, threats, or unwanted digital access from the perpetrator. These steps can help protect privacy while maintaining control over next decisions.

WHAT TO SECURE IMMEDIATELY

- Change passwords for email and banking
- Enable two-factor authentication
- Log out of all shared devices
- Update recovery email and phone number

SMARTPHONE SAFETY CHECKLIST

- Remove fingerprint or face unlock if needed
- Check app permissions
- Disable location tracking
- Watch for suspicious apps

SOCIAL MEDIA PROTECTION

- Make accounts private
- Remove unknown followers
- Screenshot abusive messages before blocking
- Disable tagging permissions

EMAIL & CLOUD ACCOUNTS

- Review login history
- Remove unknown connected apps
- Disable auto-forwarding rules

- Secure sensitive backups

STALKING & LOCATION SAFETY

- Turn off location sharing
- Check for tracking devices
- Review vehicle GPS access

PROTECTING HOME TECHNOLOGY

- Reset router passwords
- Remove access from smart home devices
- Rename Wi-Fi if identifying you

SAFE COMMUNICATION

- Use private browsing for sensitive searches
- Create a separate email for legal contacts
- Save trusted contacts under a code name

ONLINE EVIDENCE PRESERVATION

- Screenshot threats and timestamps
- Export chat histories
- Do not delete harmful messages

IF YOU SUSPECT DIGITAL SURVEILLANCE

- Switch devices before taking action
- Contact a confidential advocate
- Consider reporting if at risk

Your safety comes first. You do not need to report to protect yourself online.

