Technology Safety for Survivors

of Domestic and Sexual Violence

NEW YORK STATE
Office for the Prevention of Domestic Violence

TABLE OF CONTENTS

Disclaimer

You can be empowered through technology and have a right to access it privately and safely. This resource is a tool for survivors of domestic and sexual violence and the service providers who work with them. It contains information and instructions which should only be considered as a guide for online safety. When using information from this document, remember that any sudden changes to technology can alert an intimate partner and impact safety.

The instructions in this document cannot guarantee safety and are best used with an advocate who can help make a safety plan that is unique to your needs. To find an advocate, contact the NYS Domestic and Sexual Violence Hotline: call 800-942-6906, text 844-997-2121 or chat at opdv.ny.gov.

POWER AND CONTROL

What is Domestic Violence?

Domestic violence is a pattern of behavior used by an individual to establish and maintain power and control over their intimate partner. The behavior includes abusive tactics, threats and actions that may or may not rise to the level of criminal behavior. The tactics may include physical, emotional, financial and sexual abuse.

Domestic violence can happen to anyone. It looks different in every relationship and no one experiences it in the same way. Although it may look different, there is always an underlying theme of control. When one person tries to control their intimate partner, that isn't love; it's abuse.

What is Sexual Violence?

Sexual violence includes forms of violence where there is sexual activity without consent. This may include rape, sexual assault or sexual abuse, including vaginal or anal penetration, oral sex and genital touching. Some victims are sexually assaulted by a stranger. Most have a relationship with their attacker. It may be an intimate partner, ex, friend or family member.

What is Technology-Assisted Abuse?

Technology-assisted abuse is a tactic of abuse used to maintain power and control in an intimate relationship. It occurs when one person misuses technology to harass, intimidate, stalk and/or manipulate their partner. Technology-assisted abuse is just one of the many tactics used in a pattern of behaviors to maintain control.

When using technology, a person can often stay anonymous. They can use fake names or avatars and use spyware that goes unnoticed. This allows one person to monitor their partner's activities online and offline. When the abusive partner knows all the details of their partner's life, they only gain more control. It becomes easier to harass, stalk, threaten and isolate.

Some examples of technology-assisted abuse are:

- Hacking into online accounts and locking you out of important accounts. This may limit access to financial information or isolate you from family and friends.
- Impersonating you on online accounts, changing important information or harassing family and friends.
- Sending harassing messages repeatedly through services like cell phones, texts, messaging apps or email.
- Monitoring and tracking you by monitoring computer or cell phone, using hidden cameras or hacking GPS, etc.
- Forwarding or posting intimate images without your consent, or using them as blackmail.

Cyberstalking

Cyberstalking is a type of online harassment that uses technology to stalk. Cyberstalking may look like:

- Impersonating you or attempting to make contact using a fake online persona.
- Getting unauthorized access to personal accounts (email, social media, banking, entertainment services).
- Posting messages to online bulletin boards and discussion groups with your personal information such as home address, phone number or SSN.
- Tracking you through your phone's GPS.
- Monitoring or harassing you through social networks, game consoles, virtual classrooms, smart appliances in the home and more

Nonconsensual Pornography

Nonconsensual pornography, also sometimes known as “revenge porn,” is the act of sharing an intimate or sexually explicit image or recording of another person without their consent. Nonconsensual pornography may look like:

- Sharing images without your consent that you took and sent during an intimate relationship intending for them to remain private.
- Taking and sharing hidden recordings or images.
- Stealing private images off phones or computers and sharing them.
- Recording and sharing the recording of a sexual assault.

MALICIOUS TOOLS

With technology always changing, it is impossible to know all the available tools that someone might use to control their intimate partner. Below is a list of commonly used devices and tools that are currently on the market.

Rubber Duckie

This device looks just like standard USB drive. It steals all passwords stored inside a laptop or phone. The device can be successfully used even if the laptop is locked with a password. It only must be put in any open USB port for 15 seconds. No action is displayed on screen.

OMG Keylogger Cable

This device looks just like a standard Apple charging cable. It saves and sends all keyboard inputs (everything that is typed) like passwords or text messages from one device to another when plugged in. It can also be used to remotely send commands to someone else’s device, so someone can log in to your accounts without even being at your computer.

Malware (Software type)

Malware is software that acts like a virus. It is very affordable and frequently used. To best protect from malware, always keep system antivirus protections up to date and update all devices to the latest system version to ensure the latest security.

Malware may allow abusive partners to have remote access to your device’s camera and microphone. The malware may come through via email, when the you click on a link from an “untrustworthy source.”

Spoofing software is another type of malware. It comes in many different forms, but all are used to deceive the receiver from correctly identifying where a message is coming from. An abusive partner may use spoofing software to hide their own phone number or create a fake phone number and pretend to be someone else when making calls.

Phishing Emails

Phishing emails are designed to trick someone into sharing important and private information. They can seem very convincing, but there are several different techniques that could be used to identify phishing emails. Phishing emails are often delivered via fake log-in attempt notifications, insurance invoices or money refunds. These emails will ask you to access a link that will take you to a site which would require you to enter your email and password as verification. Some emails might only require an individual to open the link for the attacker to take control of the device.

LAN Turtle

This device allows abusers to intercept all network traffic when it is plugged into any USB port. This may be placed in a computer or a home video surveillance box. This would allow for remote access to the home video security feed or remote access to desktop and network activities like internet or cell phone searches.

Deepfake Technology

Deepfake allows someone to use an image of someone's face as a replacement on any face inside any video or image. Deepfake technology is commonly used in pornographic videos, which may then be used as a method of manipulation and revenge. Nonpornographic deepfakes are also becoming increasingly more common in separation, divorce and custody situations.

STRATEGIES FOR ENHANCING SAFETY WHEN USING TECHNOLOGY

Safety is never a guarantee for someone who experiences abuse or harassment. However, there are steps you can take to guide your safety. Below are some strategies when using technology.

Limit Publicly Shared Information

Reducing the amount of publicly shared information, like favorite restaurants and your current place of work, decreases the chances of harassment.

Guard Personal Information

It is important to know how much information is available in order to know how to protect that information. Simply use a search browser to search your first and last name and see what information is revealed.

Mute Accounts

Blocking an individual or deleting accounts may lead to further escalation. Muting an account will not notify the individual. The muting feature will just block all sent content from your feed and notifications.

Use Private Online Accounts

Using private accounts gives better control over who can message and see your online content. Harassers would not be able to impersonate your identity with photo content. Your private life will only be shared with closest friends and family.

Two-Step Verification

Upon creating online social media accounts, enabling two-step verification will ensure that any login attempts will require access to your cell phone's text messaging service or email for confirmation. Steps in the section below will teach you how to create two-step verification if you do not already use it.

Validate Connections

When receiving an email, avoid opening links from email addresses that you don't know or do not know well. Create a second email account to only use for email subscriptions and do not include personal information in case the account is taken over.

Use Camera Covers

Use camera covers on phones and laptops to block the lens when not in use. This prevents a hacker from using them to invade privacy.

CHANGE SOCIAL MEDIA SETTINGS

It's important to know how to manage safety and privacy settings on the social media platforms you use. Technology is ever-changing, and different applications regularly update their privacy settings. It is important to always read these changes as they happen. Below are some basic ways to access your privacy settings on the four most popular social media platforms: Instagram, Snapchat, Facebook and Twitter (as of October 2021).

Instagram

Set Up Private Account

Settings > Privacy > Private Account (On)

Two-Factor Authentication

Settings > Security > Two-Factor Authentication > Get Started > Enable

- Additional Methods should be left as default

Unrecognized Login Attempt

Settings > Notifications > From Instagram > Unrecognized Logins (On)

Disable Tags & Mentions

Settings > Privacy > Tags & Mentions > No One or People You Follow

Unrecognized Login Attempt

Settings > Privacy > Activity Status > Show Activity Status (OFF)

All Login History (Device model and Location)

Settings > Security > Login Activity > Confirm Logins

- Unathorized Logins will require an immediate password change

Inactive Third-Party Account Connections

Settings > Security > Apps and Websites > Active > Disable

- Any inactive third-party services like dating serivces.

Snapchat

Enable Ghost Mode

Settings > WHO CAN... > Ghost Mode (ON) > Until turned off

- Alternatively, you can also enable only certain friends to see your location under the same settings.

Two-Factor Authentication

Settings > Two-Factor Authentication > Continue > Enable

Set Up Private Mode

Settings > WHO CAN... > Contact Me > My Friends

- View story custom feature will only allow selected accounts to view stories
- See Me In Quick Add (OFF)

View All Login History, All Account Locations & Non-Deleted Talk History

Settings > My Data > SUBMIT REQUEST

- Snapchat will then send an encrypted link to the email linked with the account. There will be a 72-hour period of time in which the data is downloadable.

Facebook

Disable Precise Location Tracking

Settings > (Privacy) Location > Location Services (OFF)

- Disable Location History under the same settings

Two-Factor Authentication

Settings > (Security) Security & Login > Use two-factor authentication > Enable

- Setup unrecognized logins via the prefered method under the same settings

All Account Login History

Settings > (Security) Security & Login > Where you're logged in > See all

Set Up Private Account

Settings > (Privacy) Privacy Settings > (Privacy Shortcuts) Check a few important settings > Who can see what you share > Select Only me

- Selecting Friends will only allow friended connections to view information
- Other topics under this section will also control other privacy controls, such aswhich individuals would be allowed to Friend Request your account.

Who Can View Account Stories

Settings > (Stories) Story Settings > Story privacy > Friends or Custom

- Hide Story From... Excludes selected individuals from viewing stories
- Sharing options (Don't Allow)

Twitter

Set Up Private Account

Settings > Privacy & safety > (Tweets) Protect your tweets > Enabled

- Photo tagging disabled

Disable Public Direct Messages

Settings > Privacy & safety > (Direct Messages) Allow message request from everyone > Disabled

- Show read receipts disabled

Disable Precise Location

Settings > Privacy & safety > (Location) Precise location > Disabled

Two-Factor Authentication

Settings & privacy > Security and account access > Security > Two-factor authentication > Enable

- This task can only be preformed inside a desktop environment or a desktop version of the site on a mobile device

CHANGE CELLULAR DEVICE SETTINGS

Privacy settings can also be updated on cellular devices. Follow the instructions below to access the most important privacy settings on different smartphones.

Phones: iOS (iPhone)

Remove Unauthorized Certificates

Malicious individuals may have installed malware on your device without consent. Cell phone certificates may grant individuals complete access to certain aspects of a device remotely.

- Settings > Search bar > Trusted Certificates
  - Remove any expired or unauthorized certificates.

Remove Devices No Longer in Possession iCloud

Individuals with access to old phones still signed in may use Find My iPhone to track your movement.

- Settings > Apple ID > Remove the Device.

iMessage Settings

Disable read receipts, keep messages and audio messages set to forever.

- Individuals will not be able to see when a message is read.
- Harassment messages may be able to be used as evidence in a court of law.

Disable Shared Location with unauthorized Individuals.

- Contacts > Select the Individual > Select Stop Sharing My Location
  - This will prevent GPS tracking. When sharing GPS location with an individual, consider sharing with a time & date expiration.

Disable Location Tracking

- Settings > Search bar > Tracking > (OFF) > Ask Apps to Stop Tracking

Android OS (Samsung)

Remove Unauthorized Certificates

Malicious individuals may have installed malware on your device without consent. Cell phone certificates may grant individuals complete access to certain aspects of a device remotely.

- Settings > Search bar > Certificates > User certificates

Disable Unauthorized Admin Apps

Malicious individuals may have installed malware on your device without consent. These apps can grant complete access to the device remotely while operating undetected.

- Settings > Search bar > Device admin apps
  - Remove any unauthorized application that may seem unrecognizable to your daily use.

Disable Location Tracking

Malicious individuals may have installed malware on your device without consent. These apps can grant complete access to the device remotely while operating undetected.

- Settings > Search bar > App Permissions
  - Disable location services on any unauthorized applications that may seem unrecognizable to your daily use.

PASSWORDS MANAGEMENT

Abusive partners may convince their intimate partner to share their passwords through threats, coercion, violence or manipulation. In the beginning of a relationship, they may suggest that sharing passwords shows love and trust. If you have control over your passwords, the tips below may help you create a password that will provide the most protection from your abusive partner or ex-partner.

Do:

- Change account passwords every 12 months.
  - This helps prevent predictability.
- Avoid using the same password across multiple accounts.
  - A single account breach means all accounts that share the same password will be breached.
- Avoid using information that is directly connected to you.
  - This includes class graduation year, birthdays, relatives' names etc.
- Avoid common substitutions like the name of popular singers.
  - Bad password: EltonJohn1992NY
  - Good Password: vFQ&6OiZy%nX1za7d^wlX20
- Be cautious when using online password generators. When using these, the data trail from your device could be tracked and used in part to break into the password.
- Use the TTS Handbook as a guide to developing strong passwords.

Don't:

- Store passwords inside the cell phone's notepad app. Individuals with phone access would be able to obtain passwords without much restraint.
- Write down passwords on post-it notes or notebooks because these are easily lost. If found by other individuals, they would be able to see all the passwords in plaintext.

Recommended Electronic Password Storage Methods

Electronic password storage solutions automatically encrypt passwords to prevent anyone, other than the authorized individual, from accessing the data. Search for electronic password storage options online, do your research to make sure that it is safe, and consider:

- Services that allow two-step verifications are recommended.
- Auto fill options promote stronger passwords.

THE BENEFITS OF TECHNOLOGY FOR SURVIVORS OF DOMESTIC AND SEXUAL VIOLENCE

Technology can be scary, but it's also an incredibly important tool to help you get the help you need. Technology can empower you, breaking down isolation and assisting you with making informed decisions about well-being and safety. Technology also helps promote your independence, confidence and competence when you can access information and services. It helps you stay connected with your support systems and service providers.

Breaks Isolation

- Technology connects you to your support systems (family, friends, counselors, support groups, provider programs).
- You can access online, peer-to-peer support from others with shared experiences.
- Helps you access gender-based violence services and chatlines for safety planning, options clarification, safe temporary housing.
- You can do your own research to help identify relationship red flags, rights/options, and a variety of information about the impact of abuse.

Mobilization/Social Activism

- Technology allows you to participate in digital protests and social activism on social media.

Safety & Accountability

- Technology permits you to file a police report online (in some locations), file for an order of protection electronically and participate in court proceedings remotely.
- Assists with storing evidence.
- Helps you research accountability programs online.
- Provides access to Victim Notification apps to be made aware of changes in partner's custody status, case details, arrests, bonding hearings, etc.
- You can Google yourself to learn about your digital footprint and make appropriate changes.
- Access to danger assessment tools.
- Creates opportunities for you to use Smart devices in the home to aid with safety and document abuse.

Access

- Technology helps you access healthcare services and telehealth platforms
- It reduces barriers for those who live with disabilities, speak another language or have culturally-specific needs. It makes it possible for you to have economic stability (attend classes, work remotely, job training).
- It gives you the opportunity for Crowdfunding, if needed.

TECHNOLOGY ABUSE AND THE LAW

You may be able to get a Family Court order of protection if you are experiencing technology-related abuse, however you must prove that an enumerated family offense (EFO) was committed. The EFOs that may include tech-facilitated abuse are:

- Unlawful dissemination or publication of an intimate image
- Aggravated harassment 2nd
- Stalking 4th, 3rd, 2nd, 1st
- Identity theft 1st, 2nd, 3rd
- Coercion 2nd, 3rd

There are other criminal charges that can be brought against an abuser engaged in technology abuses. Reach out to your local law enforcement agency to file a complaint.

GET HELP

NYS Domestic and Sexual Violence Hotline
Phone: 800-942-6906
Text: 844-997-2121
Chat: opdv.ny.gov

NYS Office of Victim Services: ovs.ny.gov

NYS Address Confidentiality Program: dos.ny.gov/address-confidentiality

National Network to End Domestic Violence's Safety Net Project: nnedv.org/content/technology-safety

National Sexual Violence Resource Center: www.nsvrc.org/saam/2021/survivorresources

National Stalking Awareness and Prevention Resource Center: stalkingawareness.org

Cyber Civil Rights Crisis Line: cybercivilrights.org/ccri-crisis-helpline

Cyber Civil Rights Legal Project: cyberrightsproject.com

Federal Bureau of Investigation: www.ic3.gov/Home/ComplaintChoice

Military One Source: militaryonesource.mil/family-relationships/family-life/preventing-abuse-neglect/document-technology-misuse

Office for Victims of Crime (U.S. Department of Justice): ovc.ncjrs.gov/findvictimservices