2023

Technology Safety

for Survivors of Gender-Based Violence

NEW YORK STATE

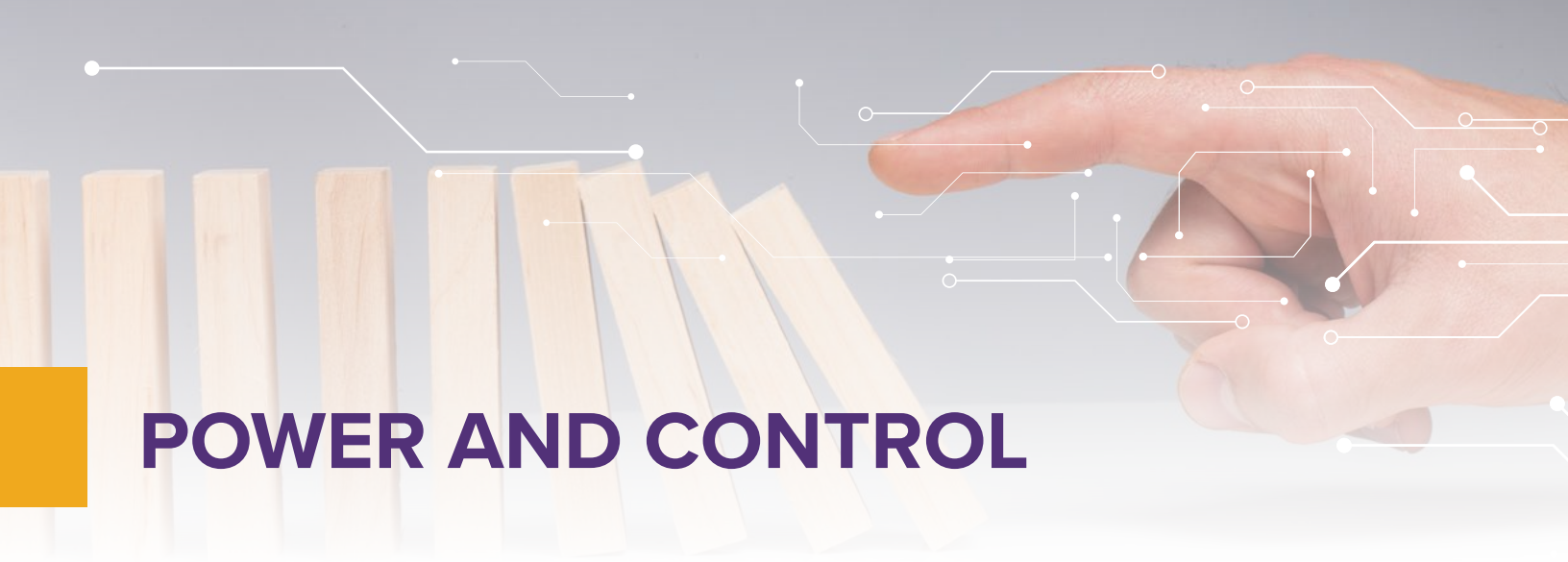
Office for the Prevention of Domestic Violence

Contents

Disclaimer:

Technology is part of our everyday lives and everyone has the right to use it privately and safely. This resource provides basic information about common digital vulnerabilities with easy steps for reducing them. When using information from this document, remember that sudden changes to settings and accounts might also activate an alert to someone misusing technology. Caution is advised.

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 near you, 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, technological, 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?

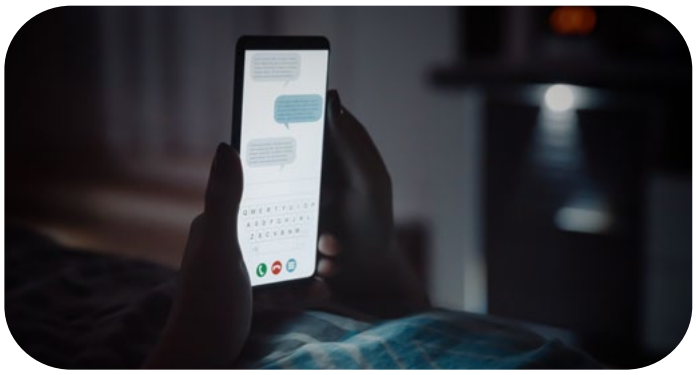
Sexual violence includes forms of violence where there is sexual activity without consent. This may include rape, sexual assault or sexual abuse, including vaginal or anal penetration, oral sex and genital touching. Some victims are sexually assaulted by a stranger. Most have a relationship with their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

What is Gender-Based Violence?

Violence or threats that happen because of someone's sex, gender, sexual orientation, gender identity or expression, or other related characteristics. Gender-based violence is an umbrella term that includes domestic violence, sex-based discrimination, sexual harassment, sexual assault, and sexual violence, and can also include stalking or human trafficking.

What is Technology-Facilitated Abuse?

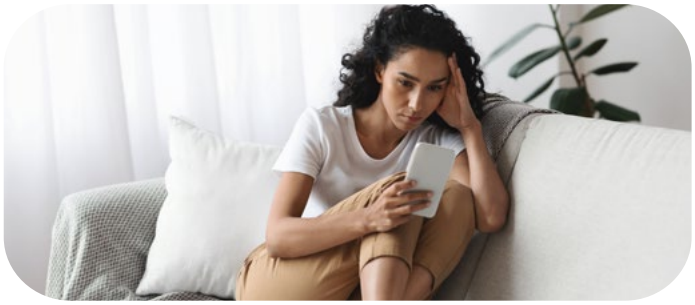
Technology-facilitated abuse is tactic of gender-based violence used to maintain power and control over another. It occurs when one person misuses technology to harass, intimidate, stalk and/or manipulate. Technology-facilitated abuse is just one of many tactics used in a pattern of behaviors to maintain control.



The misuse of technology is a tactic of abuse that is often anonymous and unnoticed. This can make it difficult to identify who is responsible. Whether this type of abuse is experienced through simple means or more complex, the experience of it is just as pervasive and traumatic as other tactics of gender-based violence.

Common examples of technology facilitated abuse are:

- → Cyberflashing: airdropping unwanted sexual images or videos to your devices.
- → Hacking into, manipulating or blocking access to accounts that harmfully impact financial status, credit, limit control of assisted devices for communication and mobility, or immigration status.
- → Repeatedly sending dozens of harassing, threatening or sexually harassing content through messaging apps, co-parenting apps and others.
- → Forwarding or posting faked images, videos, social media messages or voice mail to cause harm to relationships, for blackmail or affect the outcome of custody, divorce or other court related matters.
- → Impersonation to compromise job security, expose the victim's gender identity, expression or sexual orientation.



Cyberstalking

Cyberstalking is a type of online harassment that uses technology to stalk.

Cyberstalking may look like:

- → Creating fake personas to monitor activities and relationships through social media, gaming and other platforms.
- → Location tracking through air tags, hacked GPS, automobile smart systems or cell phone plans and apps.
- → Surveillance, following, or harassing in environments such as on-line gaming, virtual classrooms, smart appliances in the home.

Nonconsensual Sharing of Intimate Images

Nonconsensual sharing of intimate images, sometimes known as “revenge porn,” is the act of sharing an intimate or sexually explicit image or recording of another person without their consent.

This may include, but is not limited to:

- → Taking and sharing hidden recordings or images without your consent.
- → Stealing intimate images off phones or computers and sharing them.
- → Recording and sharing the video of a sexual assault.

STRATEGIES FOR ENHANCING SAFETY WHEN USING TECHNOLOGY

Before changing device settings, strongly consider the impact to your safety. Some protective actions may cause an alert, increasing risk. The free resources at the end of this guide can connect you to someone to safety plan before making changes.

Limit Publicly Shared Information

Reduce the amount of publicly shared information, like favorite restaurants and your current place of work. This limits opportunities for harassment.

Guard Personal Information

It is important to know how much of your information is available on the internet. Use a search browser to search your first and last name and see what information is revealed.

Mute or Block Accounts

Blocking an individual or deleting accounts may lead to further escalation. Instead, consider muting the abuser. Muting an account will not notify the individual. Muting will block their content from your feed and notifications without notifying them.

Two-Step Verification

Enabling two-step verification adds an extra layer of protection to online accounts. Two-step verification requires that login attempts need access to text messaging or email for identity validation.

Validate Connections

When receiving an email, avoid opening links from email addresses that you don't know or believe may be suspicious.

Use Camera Covers

Use camera covers on phones and laptops to block the lens when not in use. This may protect you from an unauthorized individual viewing you through the camera.

Software Maintenance

Install anti-virus software on all devices to scan for malware. Keep devices and apps up to date by installing the latest versions of anti-virus software.

COMMON TOOLS OF ABUSE

With technology constantly changing it is impossible to keep up with the latest tools. The list below highlights a few common tools. Please refer to the resources at the end of this guide for websites with the most up-to-date information about reducing on line risks.

Malware

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

Malware can give remote access to the device camera and microphone. Malware can be sent by email and activated by clicking on a link. Do not click on links from unfamiliar, suspicious, or untrustworthy sources.

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. Use of this software can hide a phone number or create a fake one to pretend to be someone else to the victim.

Deepfake Technology

Deepfake technology 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 as a method of manipulation and revenge. Deepfakes are also becoming increasingly common in separation, divorce, and custody situations.

Social Media

Social media can be an important tool for connection to others but also can be used to perpetrate technology-facilitated abuse. It is important to know how to manage safety and privacy settings on social media platforms.

The following resources are made available through state and national organizations specializing in technology-facilitated abuse.

- CETA Clinic to End Tech Abuse
- Safety Net Project's Technology Safety & Privacy Toolkit for Survivors

Important: *Before changing settings, consider the impact to your safety. Some changes may result in alerts that increase risk.*

Mobile Device

Mobile devices are deeply integrated into our lives. They are a critical tool for communication and connection but, yet again, can be used to perpetrate technology-facilitated abuse. A way to increase the safety of mobile devices is to update privacy settings. The National Network to End Domestic Violence's Safety Net Project has several guides to help people increase their technology safety. This resource is specifically helpful to increasing safety on mobile devices such as cell phones.

- Safety Net Project: Survivors' Guide to Phones

PASSWORD MANAGEMENT

Those who misuse technology will take advantage of their relationship with their victim to have control of passwords. A current partner might pressure the other into showing love and trust by sharing passwords. In other situations, threats or violence might be used. The tips below may help reduce risk of access by others.

Best Practices

- → Change account passwords every 3 months.
- → Avoid using the same password across multiple accounts.
  - ↘ A single account breach means all accounts that share the same password can be breached.
- → Avoid storing passwords inside the cell phone's notepad app. Individuals with phone access would be able to obtain passwords without much restraint.
- → Avoid using online password generators and managers. They can be easily accessed to interfere with your accounts, social media and other password protected site.
- → Avoid creating passwords and answers to security questions that are associated with you and easily guessed. Create incorrect answers to those questions that you can use instead.
  - ↘ This includes class graduation year, birthdays, relatives' names, etc.
- → Avoid common substitutions like the name of popular singers.
  - ↘ Less secure password: EltonJohn1992NY.
  - ↘ More secure password: vFQ&6OiZy%nX1za7d^wlX20.
- → Avoid writing 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.

THE BENEFITS OF TECHNOLOGY FOR SURVIVORS OF GENDER-BASED VIOLENCE

Everyone has the right to safe use of their technology. Technology access empowers users by giving access to resources and support, reducing isolation, assisting with making informed decisions, and supporting well-being and safety.

Breaks Isolation

- Access support systems (family, friends, counselors, support groups, provider programs).
- Access online, peer-to-peer support from others with shared experiences.
- Access gender-based violence services and chatlines for safety planning, options clarification and safe temporary housing.
- Access updated information about technology-facilitated abuse, ways to minimize vulnerabilities.

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.

Mobilization/Social Activism

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

Safety & Accountability

- Assists with storing evidence.
- 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.

TECHNOLOGY-FACILITATED ABUSE AND THE LAW

Technology-facilitated abuse may rise to the level of a crime or a violation of NYS law. Some examples of possible criminal acts are:

- Downloading surveillance apps or software without your knowledge or consent.
- Posting or distributing intimate images or videos without your consent.
- Threatening to share intimate images or videos with colleagues, family, friends, court officials as a form of blackmail.
- Sending dozens or hundreds of harassing messages or content through social media, text messages or other means.
- Accessing social media accounts, financial and medical accounts, etc. without your permission.

To explore your rights and legal options, speak with a victim advocate, an attorney, or you can report these actions to the police for them to investigate to determine if a crime was committed. It is important to know how much of your information is available on the internet. Use a search browser to search your first and last name and see what information is revealed.

GET HELP

NYS DOMESTIC AND SEXUAL VIOLENCE HOTLINE

TEXT: **844.997.2121**

CALL: **800.942.6906**

CHAT: **OPDV.NY.GOV**

Free. Available 24/7. Confidential support in most languages.

NYS OFFICE OF VICTIM SERVICES:
ovs.ny.gov

NYS ADDRESS CONFIDENTIALITY PROGRAM:
dos.ny.gov/address-confidentiality

CLINIC TO END TECH ABUSE, CORNELL UNIVERSITY:
ceta.tech.cornell.edu/aboutus

CYBER CIVIL RIGHTS CRISIS LINE:
cybercivilrights.org/ccri-crisis-helpline

CYBER CIVIL RIGHTS LEGAL PROJECT:
cyberrightsproject.com

FEDERAL BUREAU OF INVESTIGATION:
ic3.gov/Home/ComplaintChoice

NATIONAL NETWORK TO END DOMESTIC VIOLENCE'S SAFETY NET PROJECT:
nnedv.org/content/technology-safety

NATIONAL SEXUAL VIOLENCE RESOURCE CENTER:
nsvrc.org/saam/2021/survivorresources

MILITARY ONE SOURCE:
militaryonesource.mil/preventing-violence-abuse/unhealthy-relationships/technology-misuse-and-your-relationship

NATIONAL STALKING AWARENESS AND PREVENTION RESOURCE CENTER:
stalkingawareness.org

OFFICE FOR VICTIMS OF CRIME (U.S. DEPARTMENT OF JUSTICE):
ovc.ojp.gov/directory-crime-victim-services