Overview

Technology Abuse is a form of controlling abusive behavior that involves the use of technology to stalk, harass, or threaten another person. It includes the behaviors on digital platforms that compromise someone's privacy and safety, causing them emotional, physical, and reputational harm.

Tech abuse can include:

- Image-based abuse
  - □ **Non-consensual Image Sharing** ('revenge porn') - The sharing of someone's sexual images without their permission.
  - □ **Sextortion** - Blackmailing, or threatening to force, someone to send sexual images.
  - □ **Deepfake** - An image that has been edited and made to falsely appear real, often with sexual content.
- **Cyberstalking** - The unwanted pursuit, harassment, or contact of others using electronics.
- **Doxing** - The public release of private and sensitive personal information about someone without their permission.
- **Monitoring and surveillance** - Using technology to control someone's behavior by tracking their location, taking pictures, eavesdropping, and gaining access to their email, social media, or other online accounts. This can also include monitoring someone's personal health information, like their period, by apps or other tech.

97% of victim service providers surveyed in 2014 indicated that victims who seek their services are being harassed, monitored, and threatened by someone misusing technology.

National Network to End Domestic Violence

Resources

There are many organizations that specialize in supporting survivors of tech abuse. They can help provide you with technical support and knowledge, support you in reporting abuse to platforms, and connect you with resources for specific types of tech abuse.

The Cyber Helpline
www.thecyberhelpline.com

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

NCMEC's Cyber Tipline - Child Sexual Abuse Material Removal Support
www.missingkids.org/gethelpnow/cybertipline

THORN's Non Consensual Image Sharing Removal Support
www.stopsextortion.com/get-help

Human Trafficking Hotline
www.humantraffickinghotline.org

End Tech Abuse
www.endtab.org

SALI
www.mcasa.org/survivors/sali

Find your local Rape Crisis Center:
www.mcasa.org/survivors/find-a-rape-crisis-center

MCASA
Maryland Coalition Against Sexual Assault

MCASA is open during the COVID-19 crisis - we are here for you.

mcasa.org | 301-328-7023
info@mcasa.org
P.O. Box 8782
Silver Spring, Maryland 20907

Preparation of this document was supported by grant number #PHPA-G3132 and reprinted with support by the Evidence for Sexual Violence Prevention (CE # 1 9- 1 902) and the MDH Rape & Sexual Assault Prevention Programs, grant #PHPA-1740, both awarded by the Maryland Department of Health. The opinions, findings, and conclusions expressed in this document are those of the author(s) and do not necessarily represent the official position of policies of the Centers for Disease Control (CDC) or the Maryland Department of Health.

9/2022

Technology & Safety

MCASA
Maryland Coalition Against Sexual Assault

Tech Safety Tips

While tech abuse is becoming increasingly common, we can all better understand our own technology use and take steps to increase our privacy and safety.

Stalkerware & Location Tracking

Stalkerware and Spyware are apps, software programs, or devices that allow another person to monitor and record the activities of someone's computer or phone. These tools can all be used for surveillance, harassment, and stalking without the user's permission. To combat the abuse of stalkerware, we can all:

- Remove Exchangeable Image File Format (EXIF) information from shared photos. This is the basic information that is created and stored by the camera whenever you take a photo, like the location and time.
- Manage our Bluetooth and Wifi settings.
- Watch for tracking devices on our personal items.

Phones

Smartphones can store sensitive information, track locations, and provide easy access to our personal accounts. This creates a potential safety risk and space for someone to control and harass survivors. To stay safe on our phones, we can all:

- Turn off location tracking and sharing, or be careful with whom we share this information.
- Manage our 'Find My Phone' settings.
- Check and manage our location sharing through social media and other apps.
- Turn off Bluetooth and Wi-Fi settings when not in use.
- Enable passcodes and FaceIDs on our devices.

IoT & Connected Devices

The Internet of Things (IoT) are devices connected to each other or an app that controls them. Most IoT devices are connected to each other through the internet or bluetooth. Items like baby monitors, smart watches, and home security systems can be used for surveillance as a way to control behavior by taking pictures, tracking activity, eavesdropping, and gaining access to email. To stay safe while using IoT devices, we can all:

- Learn about the built-in security options of individual devices.
- Change the default settings and passwords, including router and network settings.
- Turn devices off when not in use.
- Monitor our accounts for unusual activity.

Online Privacy & Safety

The Internet offers countless ways to stay connected and create virtual communities, but can be another platform for someone to monitor, stalk, and harass others. To stay safe online, we can all:

- Use unique passwords and consider using two-step authentication to login when available.
- Search ourselves online to be aware of what information is publicly available.
  - □ If we find personal info we don't want online, we can 'De-Dox' ourselves through Data Broker Opt Outs to remove it.
- Use different usernames for different websites so accounts are not easily linked.
- Delete our Wi-Fi network history as phones, tablets, and laptops may record all Wi-Fi networks we connect to.
- Understand the privacy settings and policies of the websites we use.

Social Media

To stay safe on social media, we can all:

- Review our privacy settings, security settings, and notification settings.
  - □ Manage who can see what we post and share.
  - □ Manage who can see our location (Snap Maps, Check ins, Geotags).
- Be mindful of how much personal information we post.
- Know and manage our friends - be cautious when accepting new friend and follow requests.
- Set clear boundaries with family, employers, and friends about what they can post online about us.

Tech & Safety Assessment

If you are experiencing tech abuse, these questions can help you think about your safety:

- Prioritize Your Personal Safety:
  What are your current safety concerns?
- Narrow Down Which Technology is Being Abused:
  What has made you feel concerned and unsafe?
- Measure your Understanding of the Technology:
  How do you think this abuse is happening? What information does someone have access to that they shouldn't?

Assessement adapted from the National Network to End Domestic Violence Safety Net Project

Getting Support

We should all be able to access technology freely and safely and be online without limitations or fear. If someone is impacting your tech safety, this is tech abuse. It is never your fault, and professional help may support you through your healing process. If you are experiencing tech abuse, you might consider:

- Reaching out to trusted family or friends who can offer emotional support, help you understand your options, and support your choices.
- Calling your local Rape Crisis Center to speak with advocates who can answer questions, provide emotional support, or just listen.
- Keeping screenshots and a log of all communications (text messages, social media posts, emails, phone call logs, voicemails, etc.) with, and from, the person causing harm.
- Reporting the tech abuse to the police.

Misuse of technology to annoy, stalk, harass, or abuse someone is a crime in Maryland. Survivors of tech abuse may be able to pursue both criminal actions and civil legal actions, like peace and protective orders, to stop communications from the person misusing tech. You can contact the **Sexual Assault Legal Institute** for more information on legal support at **301-565-2277**.