TECH SAFETY

A victims safety is our priority, this includes their online safety. Before they just throw away their device, consider some abusive individuals may escalate the controlling and dangerous behavior if they feel they've lost access them. Some survivors choose to use a safer device for certain interactions, but also keep using the monitored device as a way to collect evidence.

Techsafety.org is an excellent resource. This page has been modified from information provided on their website. Please visit their site for more in depth details on how to keep yourself safe. Here are some things to consider for your electronic and mobile devices.

Using a safer or different device the abusive person hasn't had access to.
Trust your instincts. If it seems like the person knows too much about you, they could be getting information from a variety of sources, like monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online.
Look for patterns. Take some time to think through what kind of technology may being used to stalk, monitor, or harass you. For example, if the abusive person has hinted they are watching you, think about what they know. Do they only know what you are doing in a certain area of your home? If so, there may be a hidden camera in that room. If you suspect you're being followed, is it just when you're in your car or is it also when you are on foot? If it's just in your car, then there may be a device hidden in your car. If it's everywhere, it may be something you are carrying with you, such as your phone or a tracker in your bag.
Document the incidents. Documenting a series of incidents can show police or the court a pattern of behavior that fits a legal definition of stalking or harassment. Documentation can also help you see if things are escalating and help you with safety planning.
Report the incidents. Consider reporting to law enforcement and/or the website or app. If the behavior violates the platform's terms of service, the content may be removed or the person may be banned. Reporting content may remove it completely so it should be documented prior to reports for evidence.

<u>Steps to Increase Security</u>

- **Change passwords, passcodes and/or usernames to non-identifying. Don't forget your social media.**
- **Check your devices & settings for:**
  - Other devices or accounts aren't connected to yours
  - Device-to-device access, like Bluetooth or Air-drop is turned off when not using.
  - Spikes in data usage –may indicate monitoring software such as spyware in use.
  - Unused or unfamiliar apps
  - Location sharing in apps and on devices – if location tracking is suspected on your vehicle, contact a mechanic or law enforcement for an inspection
  - Accounts automatically logging you in
  - Remote access features on your computer
  - File sharing
- **Get a new device.** A pay-as-you-go phone is a less expensive option. Put a passcode on the new device, and don't link it to your old cloud accounts like iCloud or Google that the person might have access to.

- **Consider cameras and audio devices such as Google Home, Alexa or security systems.**
- **Log out of accounts and quit programs.**
- **Don't click on unknown or suspicious links.**
- **Use a VPN (Virtual Phone Number) to keep your number private.**
- **Delete sensitive information from your devices like text or voice messages and emails.**
- **Use anti-virus/anti-spyware on all your devices.**
- **Take care when using "personal safety" apps.** Several of these apps are designed and marketed specifically to survivors of violence. Before relying on any safety app in an emergency, be sure to test it out with friends and family to be sure it works.
- **Don't root or jailbreak your phone. (**Removing the manufacturer and carrier's restrictions) This makes the phones more vulnerable to spyware and malware.
- **Create a non-admin user for everyday computer use.** Some malware and "hacks" require administrative access to your computer. If you are signed in as a non-administrator and set it up so a non-administrator account cannot install software, it won't install even if you accidentally click on a link with malware.
- **Turn on firewall protections.**
- **Limit the information you give out about yourself.**
- **Control your offline & online privacy.** The Survivor Toolkit at TechSafety.org has Online Privacy & Safety Tips, including more information about changing settings on your mobile devices, social media accounts such as Facebook and Twitter, and your home WiFi network.

<u>Signs of possible spyware include:</u>

- **Rapid battery loss**
- **Device turning on and off**
- **Spikes in your data usage**
- **Abuser's suspicious behavior**

<u>Remove spyware by:</u>

- **Factory reset**
- **Reinstall apps manually from a new your app store**
- **Not connecting to old backups**

<u>Resources to check out:</u>

- **Techsafety.org**
- **VineLink App or Vinelink.com (Sends prison inmate status updates)**

STALKING

For victims of stalking, it can be critical to maintain a log of stalking-related incidents and behavior, especially if they choose to engage with the criminal or civil justice systems. Recording this information will help to document the behavior for protection order applications, divorce and child custody cases, or criminal prosecution. It can also help preserve your memory of individual incidents about which you might later report or testify. The stalking log should be used to record and document all stalking-related behavior, including harassing phone calls, text messages, letters, e-mail messages, acts of vandalism, and threats communicated through third parties. When reporting the incidents to law enforcement, always write down the officer's name and badge number for your own records. Even if the officers do not make an arrest, the victim can ask them to make a written report and then request a copy for their records.

Important note: Since this information could potentially be introduced as evidence or inadvertently shared with the stalker at a future time, they should not include any information they do not want the offender to see. Attach a photograph of the stalker, photocopies of restraining orders, police reports, and other relevant documents. Keep the log in a safe place and they should only tell someone they trust where the log is kept. Documenting stalking behavior can be a difficult and emotionally exhausting task.

Montana Annotated Code, Title 45. Crimes, Chapter 5, Part 2 reads:

45-5-220. Stalking -- exemption -- penalty. (1) A person commits the offense of stalking if the person purposely or knowingly engages in a course of conduct directed at a specific person and knows or should know that the course of conduct would cause a reasonable person to:

(a) fear for the person's own safety or the safety of a third person; or

(b) suffer other substantial emotional distress.

(2) For the purposes of this section, the following definitions apply:

(a) "Course of conduct" means two or more acts, including but not limited to acts in which the offender directly or indirectly, by any action, method, communication, or physical or electronic devices or means, follows, monitors, observes, surveils, threatens, harasses, or intimidates a person or interferes with a person's property.

(b) "Reasonable person" means a reasonable person under similar circumstances as the victim. This is an objective standard.

(c) "Substantial emotional distress" means significant mental suffering or distress that may but does not necessarily require medical or other professional treatment or counseling.

(3) This section does not apply to a constitutionally protected activity.

(4) (a) Except as provided in subsection (4)(b), for the first offense, a person convicted of stalking shall be imprisoned in the county jail for a term not to exceed 1 year or fined an amount not to exceed $1,000, or both.

(b) For a second or subsequent offense within 20 years or for a first offense when the offender violated any order of protection, when the offender used force or a weapon or threatened to use force or a weapon, or when the victim is a minor and the offender is at least 5 years older than the victim, the offender shall be imprisoned in the state prison for a term not to exceed 5 years or fined an amount not to exceed $10,000, or both.

(c) A person convicted of stalking may be sentenced to pay all medical, counseling, and other costs incurred by or on behalf of the victim as a result of the offense.

(5) Upon presentation of credible evidence of violation of this section, an order may be granted, as set forth in Title 40, chapter 15, restraining a person from engaging in the activity described in subsection (1).

(6) For the purpose of determining the number of convictions under this section, "conviction" means:

(a) a conviction, as defined in 45-2-101, in this state;

(b) a conviction for a violation of a statute similar to this section in another state; or

(c) a forfeiture of bail or collateral deposited to secure the defendant's appearance in court in this state or another state for a violation of a statute similar to this section, which forfeiture has not been vacated.

(7) Attempts by the accused person to contact or follow the stalked person after the accused person has been given actual notice that the stalked person does not want to be contacted or followed constitutes prima facie evidence that the accused person purposely or knowingly followed, harassed, threatened, or intimidated the stalked person.

History: En. Sec. 1, Ch. 292, L. 1993; amd. Sec. 11, Ch. 350, L. 1995; amd. Sec. 1, Ch. 344, L. 2003; amd. Sec. 2, Ch. 255, L.