OHIO VICTIM
OVWA
WITNESS ASSOCIATION

Cybersafety Guide for Crime Victims

December 2020

Contents

Preface & Purpose

ACKNOWLEDGMENTS

OVWA recognizes the need for crime victims to have guidance to protect their safety when using technology. Cybersafety is not a choice but a necessity in today's world with the consistent use of technology to meet our daily needs.

Extensive research was done to ensure that information in this guide is accurate and reflects the needs of crime victims. Some of the material was adapted from the following resources:

Technology Safety & Privacy: A Toolkit for Survivors. Produced by the National Network to End Domestic Violence.

Howell, Elaine. *"Don't Get Doxxed: Tell Data Brokers You're Opting Out".* UCLA IT Services, Feb 23, 2017, www.it.ucla.edu/news/dont-get-doxxed-tell-data-brokers-youre-opting-out

Using Technology to Hurt Others. Produced by the Rape, Abuse & Incest National Network (RAINN), www.rainn.org/safe-tech

How to Gather Technology Abuse Evidence for Court. Written by Kaofeng Lee, Ian Harris, the Safety Net Project at the National Network to End Domestic Violence (NNEDV) in partnership with the National Council of Juvenile and Family Court Judges and the Resource Center on Domestic Violence: Child Protection and Custody

Special Thanks

OVWA wishes to extend a special thanks to our content expert, Bill Wagg, Client Care Specialist with thinkCSC. For central Ohio's businesses, government, and education communities, thinkCSC is an IT services firm that invests in their clients' success for over 25 years. To learn how thinkCSC can help your business, please visit their website at www.thinkcsc.com.

As we become more and more connected, we become more vulnerable to cyberattacks. From smart refrigerators, connected thermostats, and IP video cameras, everything can be breached. And every day, there is a new breach. Cybersecurity should be on everyone's mind, but Bill Wagg lives and breathes it, maintaining a singular focus on keeping organizations safe and encouraging everyone to be more proactive about keeping data safe.

Bill's unique blend of coach, teacher, and evangelist of all things cybersecurity fuels his passions. Helping organization maintain data security while protecting the privacy of their clients and end users drives Bill. He spends much of his time educating organizations on how to adhere to both security regulations and best practices around cybersecurity and provides countless trainings to organizations to help them be more cybersecure.

For the last seven years, Bill has worked with thinkCSC clients and vendors to improve their cybersecurity knowledge and believes that every person has a part of play in improving data security. Every business needs a policy and plan in place to protect them not just from today's threats but from tomorrow's threats, too. With 53 different security certifications, Bill is in an excellent position to help ensure every organization has access to cutting-edge cybersecurity solutions.

ACCESSIBILITY STATEMENT

The authors and partners of this publication believe in accessibility for all individuals. This document is available in alternative formats upon request to OVWA. Contact information for OVWA can be found on the last page of this guide. Please allow for sufficient time to arrange such accommodations.

ELECTRONIC ACCESS

This guide can be downloaded from OVWA's website at www.ovwa.org/best, under OVWA Publications.

DISCLAIMER

The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the policies or position of any agency. Examples provided in this publication are simply examples. Assumptions made are not reflective of any agency or victim rights organization. The following information has been collected from extensive research, learned experiences, and expert opinion.

This guide was supported by grant number 2021-VOCA-134145796 awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice through the Ohio Attorney General's Office. Victims of federal crimes will be served.

Introduction

If you are reading this, you are likely going through a difficult situation in which your safety is a top priority. There are many things to consider in planning for your safety and this publication will provide some tips and guidelines for you to consider when using technology. Cybersafety refers to the ways in which you can protect your personal information on technological platforms. Cybersafety is the safe and responsible use of information and communication technology. It is about keeping information safe and secure but also about being responsible with that information.

This guide is intended to be a starting point at this critical time in your life. Please know that you are not alone you do have support. Although sometimes you may feel very alone, please reach out to supportive family, friends, colleagues, and trusted professionals. We have included phone numbers of both state and national organizations for help if you are the victim of a crime. The impact of cyber insecurity is very real. Offenders can exploit this leaving you feeling threatened and afraid. The goal of this guide is to provide you with some beginning, and hopefully lasting, steps that you can take to empower yourself. We encourage you to use this guide with a trusted professional or advocate as you may need to develop a safety plan specifically for cybersafety.

SAFETY TIP

Throughout this guide, one of the Safety Tips we offer is to complete an internet search on how to disable certain settings within your specific technological devices. Manufacturers of cell phones, computers, laptops, and tablets all have different ways of personalizing settings therefore, an internet search may be necessary to complete these tasks. If you should choose to act on these Safety Tips, please make sure you are completing an internet search on a device you do not believe to be compromised.

A WORD ABOUT YOUR PRIVATE INFORMATION

When you have become a crime victim, you may find that many agencies and organizations are asking for your personal information. Suddenly you may have an overwhelming amount of phone calls, appointments and "official "meetings with persons that are intended to help you through this event. It is important to remember that you have choices about what information to share, how much and with whom. If you sign a release of information to let some of these officials share your information with others, you may cancel that at any time. These "officials" may need certain information to help you stay safe, but it is ultimately your choice.

If you are attempting to remain in an undisclosed location, consider applying to the Safe at Home program through the Ohio Secretary of State. Safe at Home is an address confidentiality program that allows victims of domestic violence, human trafficking and other crimes, as well as members of their household, apply for a substitute address that they can use to shield their residence from public record. You may find out further

information about this address confidentiality program by visiting the Ohio Secretary of State website at www.ohiosos.gov/secretary-office/office-initiatives/safe-at-home.

DOCUMENTING ABUSE

If you are a victim in a criminal case against someone it may be helpful to retain documentation from your tech devices to aid in the criminal case. Phone call records, text messages, tracking apps, computer activity, or evidence of unauthorized use of images are just some forms of documentation that outlines the harassment, monitoring, or threats you are enduring.

Within this guide, you will find guidance on how to document and retain this information for your own purposes or for law enforcement. Many times victims of crime are questioned as to why they don't just change their number or delete social media accounts when harassment is occurring. You may want to keep social media accounts for various reasons, such as staying in touch with family and friends. It is important to monitor what is happening on these accounts to further help assess your own safety risk. After leaving social media sites or changing your number, offenders could escalate their behavior to more vigorously attempt to gain information about you. Leaving social media sites also limits you access to others in case of an emergency. For these and many other reasons, you may decide to remain on your devices and social media, but in a safer way for you.

You will see that we mention several times throughout this document how to capture harassing and disturbing comments and pictures. To capture what is happening, it is important how you gather this information. Here are a few tips on how to successfully document abuse through screenshots:

HOW MANY?

Capture more than one message. It may be necessary for you to capture an entire conversation showing the extent of abuse from the offender. Most of the time a single text message is not enough to show that something is wrong. Because stalking and harassment are a series of interactions, you will want to try and capture all of the messages that can help provide a solid background to your experience.

WHO?

When capturing information from a computer, tablet, or phone through pictures, it's also very important that you **capture who sent the message.** You can show this by capturing the offender's name, phone number, email address, and any other identifying information. The more information the better.

WHEN?

If possible, try to **capture the date and time** the message was sent. This can be easy to do with emails because each email is time stamped and dated. If it was a text message, you may need to tap or slide on the message to show the date and time that it was sent. When taking a picture of a computer or tablet screen you can make sure you capture the date and time at the bottom or top of the screen.

FILE.

As a second layer of security, you can use a **documentation log** to show when, where, and who has been hurting you. Please see the documentation log here at the end of this guide.

Assessing Your Current Level of Safety

Let's look at indicators that your safety could be compromised by someone monitoring your activities through technology. In this section, you will learn the many ways someone could be getting information about you and ways to prevent this from happening.

Please keep in mind that if you find monitoring, tracking or other programs on your tech devices and you remove those, the offender could will realize the program has stopped working. In some cases this could lead to the offender becoming angrier and react by seeking out different ways of getting your information, which can put your safety at an increased risk. If you believe your safety is at risk, please take the opportunity to begin safety planning or add cyber safety to an already existing safety plan with your advocate or trusted professional.

It is important to remember that there may not be an obvious sign that your technology is being monitored. However, here are a few things to look for if you believe someone is monitoring you.

- Your phone's battery drains faster than usual, or it is slow to turn on or off.
- You hear unusual sounds or clicks while talking on the phone.
- Someone is aware of details about you or places you will be even though you did not disclose that information to anyone.
- You see an app on your phone, computer, laptop or tablet that you did not download.
- Someone has had physical access to your phone or computer and that person now has information that you did not disclose to them.
- There are unknown charges on your cell phone bill.

Phone Surveillance

CELL PHONE TRACKING

Mobile phone tracking is a process for identifying the location of a mobile phone, whether stationary or moving. If someone has had physical access to your mobile phone or account and you are being harassed or monitored, there is a chance they are accessing your information through your phone in a number of ways.

SAFETY TIPS

- **Put the mobile phone account in your name** and change your user name and passwords so that only you have access to account records
- Look at the apps on your phone and **delete any app that you did not personally download.** Google those apps that you are unsure about. If you are still noticing odd battery drain or start up and shut down delays, consider performing a factory reset on your phone.
- If you are documenting harassment or abuse on your phone, a factory reset could cause you to lose evidence. **Consider getting a second phone for daily use** until you no longer need to preserve this evidence.
- **Lock your cell phone** with a pass code and do not share the pass code with anyone.
- **Log out of apps after each use.**
- **Turn the Bluetooth off** on your cell phone when it's not in use.

Account records

Many cell phone providers keep records of calls and texts to and from your phone that can be accessed through your account or by making a records request to the cell phone provider. If you share an account with a person that is harassing, monitoring or stalking you, they have access to all of this information.

Tracking Apps

Tracking apps have built-in functions that can track not just a phone's location but other data found on the targeted device. This type of software is also referred to as "spy apps". Some examples of these apps are Find my Phone, Find my Mobile, AT&T Secure Family, Google Family Link, Verizon Smart Family, and Sprint Family Locator. These are all tracking apps that look innocent and can be used to keep people safe but can be used for monitoring victims of crime as well.

Other Tracking Apps

Hundreds of tracking apps are available with a simple search online. Some of these operate in "stealth" mode, which means you cannot see this app when doing your own search on your phone. Some apps have the ability to actually record all text messages, actual phone calls, and some can connect live to conversations on the phone as they are happening, in real time.

SAFETY TIPS

- **You are able to remove geotagging from your photos on your phone.** You can Google this information for specific instructions for your particular phone. When doing an internet search, make sure to use a system that you do not believe to be compromised.
- When taking pictures with friends and family, **ask them to not tag you** in a picture or reference your location in a picture posted on the internet.

GEOTAGGING

Geotagging is the process of adding geographical identification data to various media such as photographs, videos, and websites. A geotagged photograph is a picture that is associated with a location. Your pictures in many apps or mobile systems are "tagged" with the time, date, and location that the photo was taken. If a picture is then sent to another person, shared online, or on social media, this information goes along with it and can be seen by another user. If an offender has access to one of your pictures that is online, they may be able to gain the location the photo was taken by doing a simple Google reverse image search online. More information about this can be found in the Social Media section of this guide.

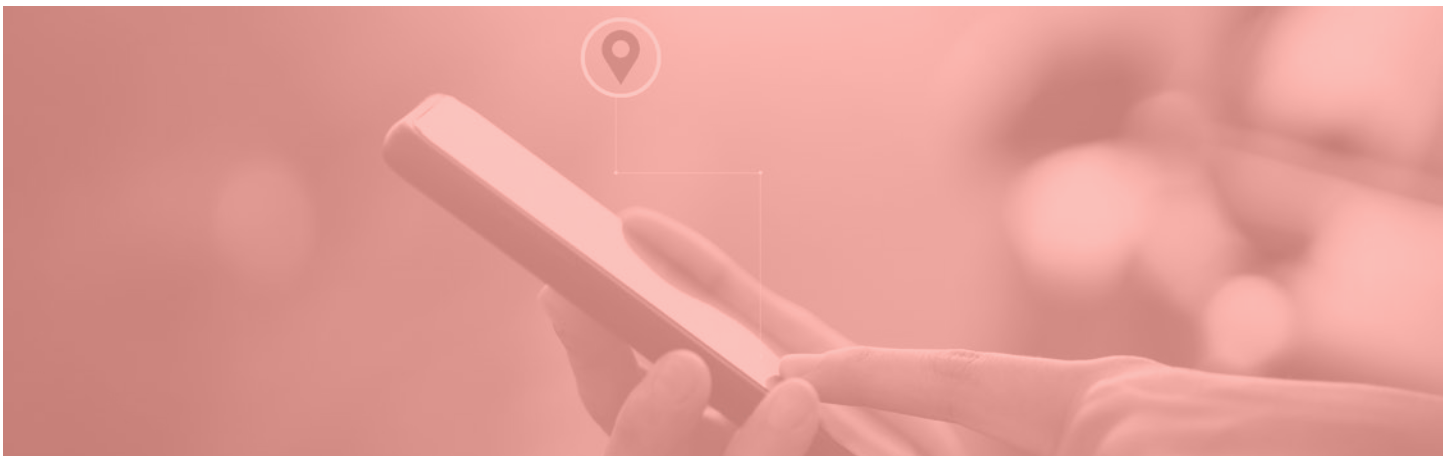
GLOBAL POSITIONING SYSTEM (GPS) TRACKING

You may be familiar with the idea of someone placing a GPS tracking device on a car in a hidden location. However, GPS tracking systems can be less than an inch long and can be attached to anything—a purse, keys, children's toys or phones, etc. GPS tracking devices are routinely sold pre-placed on pet collars and shoes.

SAFETY TIP

- **Turn off your location services on your phone and/or tablet for each app.** You can find instructions to do this for your particular phone online with an internet search. Remember, anytime an app asks for permission to access your location and you agree, your device reverts to the location being on.

Global Positioning System (GPS) tracking units are navigation devices normally carried by a moving vehicle, person, or animal. Your personal phone has as a tracking system. Almost every smart phone and many flip phones today have a built in locator. Anything you do online could potentially reveal your location if someone has taken the time to research how to locate this information. If you use Google and Gmail and your location is enabled, you can access every location your phone (you) has been by doing a simple Google location history search. Even if you have physically disabled this on your phone, each new app that asks if it has permission to use your location actually **TURNS IT BACK ON.** Additionally, if you use Google and have your location settings enabled, anyone with your user name and password for your Gmail account can access your **Google Location History.** This information can provide your location 24 hours a day, seven days a week unless your phone is turned off.



Computer Monitoring

TRACKING

As with your mobile device, software exists on computer hard drives that can track your computer activity. If the offender has physical or electronic access to your computer, user information, or log-in credentials, you can be tracked. Your internet searches, documents, photos and passwords used on your computer is then at risk. However, legitimate reasons can exist for this software. Employers may use it to monitor their employees on work issued devices and family members may use it to monitor the location of their loved ones. However, these same monitoring platforms can be used for criminal purposes, too.

Every device that accesses the internet has what is called an internet protocol (IP) address. An IP address is a number assigned to each device connected to a computer network and uses the address for communication. Additionally, if someone has access to your computer's IP address, there are ways to narrow down the physical location of your computer to city and state.

Video/Audio

If your computer, laptop, or tablet has a camera and/or speakers your systems may be vulnerable. There are programs that can allow someone to view you using your computer via the video camera on your computer or through audio.

Malware and Spyware

Malware is an umbrella term for any type of malicious software that is intentionally designed to cause damage to a computer or a computer network. A wide variety of malware exists and you may know it best as computer viruses. Spyware is a type of malware that gathers information about a person or a business without their consent or knowledge and steals internet usage data and personal sensitive information.

SAFETY TIPS

- **Make sure you have a good security program** on your computer and run this program periodically to ensure there are no malware, spyware or other unsafe programs on your computer.
- **Review the list of programs** on your computer or device and look for any unknown programs.
- **Consider taking your computer to a tech repair location** for removal of any unwanted programs.
- If you believe the offender may be computer savvy enough to try and track your computer's physical address through the IP address, **consider getting a Virtual Private Network or VPN.** A VPN creates a private connection to the internet and distorts the IP address so it cannot be tracked.
- If the offender has physical access to your computer, **consider using a different computer** and changing all of your passwords used on the computer.
- **You can block the video camera** on your computer by putting thick tape over the lens or disabled in Settings on your computer. Your microphone can be turned off through Settings as well.

BROWSER HISTORY

Delete your browsing history if the offender has current access to your computer. The Ohio Safe at Home Program suggests the following:[1]

"Computers can track information like websites you have visited and emails you have sent. If you are in danger, try to use a safe computer that the person you fear cannot access. The following are instructions on how to delete your browsing history using different browsers."

GOOGLE CHROME:

1. Click on the dropdown menu in the top right corner.
2. Click on History
3. Click on History again
4. Click on Clear Browsing Data
5. Use the drop down menu to select how far back to delete ("the beginning of time" deletes all)
6. Click on Clear Browsing Data

GOOGLE CHROME (DELETING SPECIFIC ITEMS):

1. Click on the dropdown menu in the top right corner.
2. Click on History
3. Click on History again
4. Mark a check mark next to entries you want to delete
5. Click on Remove Selected Items at the top

INTERNET EXPLORER:

1. Click on Tools
2. Select Delete Browsing History
3. Click Delete

INTERNET EXPLORER (DELETING SPECIFIC SITES):

1. Click on the Favorites button (Star button)
2. Select the History tab
3. Right click specific site and click Delete

SAFARI:

1. Click the Safari Tab
2. Select Reset Safari
3. Check Clear History
4. Click on Reset

SAFARI (DELETING SPECIFIC ITEMS):

1. Click on the History Tab
2. Click Show History
3. Right click on the item and click Delete

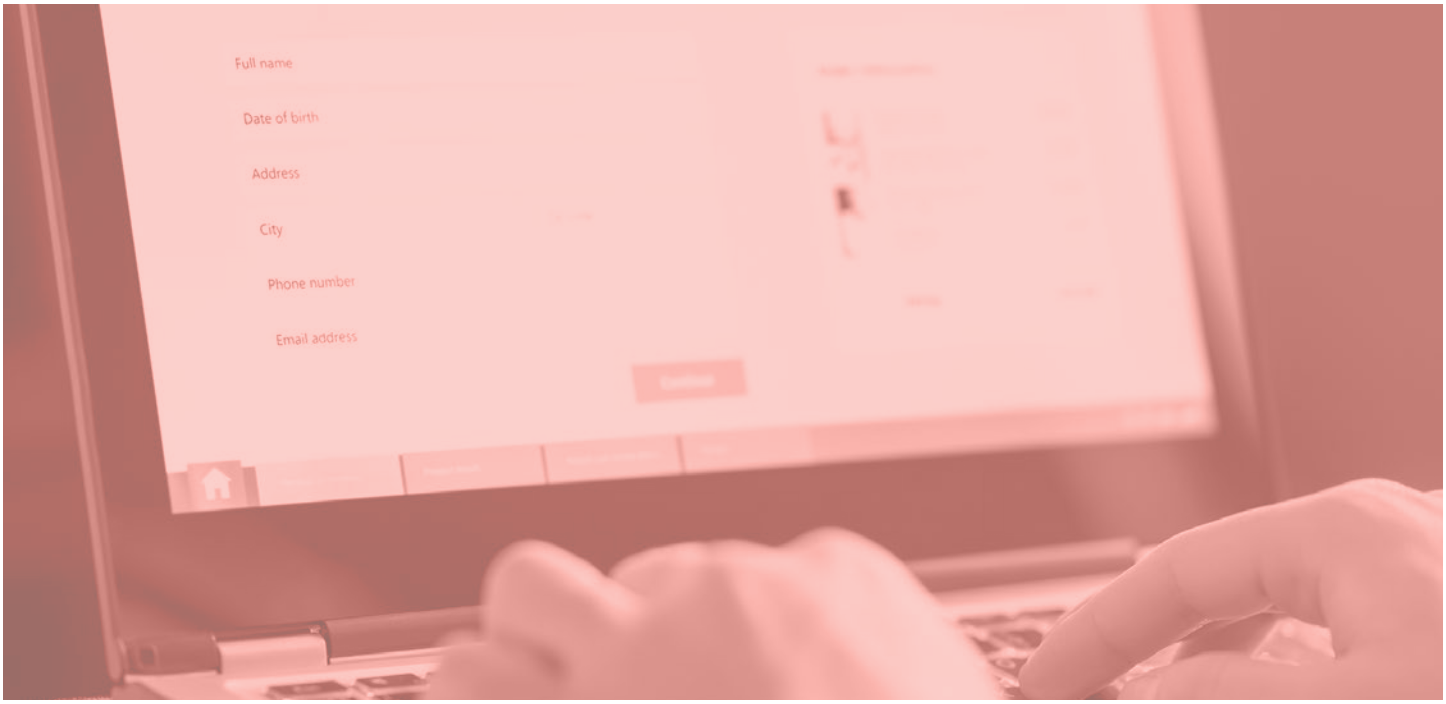
FIREFOX:

1. Using your keyboard, hit Control, Shift and Delete at the same time
2. Use the drop down menu to choose which time range you would like to delete
3. Click Clear Now to confirm

FIREFOX (DELETING SPECIFIC ITEMS):

1. Click the Menu button
2. Select Settings
3. Click Privacy
4. Click Clear Now
5. Check the items you want to clear
6. Click Clear Data

[1] www.ohiosos.gov/secretary-office/office-initiatives/safe-at-home/victims/



DATA BROKERS

Data brokers are companies that collect personal data from many different sources. Information like voting records, change of address, court records, social media, internet browsing history and either sell your information to other companies or use the information as a paid service for anyone to access. Websites like White Pages, People Search, Intelius, and Spokeo are examples of recipients of your information. An offender can easily use this paid service to obtain the information already collected about you.

SAFETY TIPS

- **Most important: Opt out of broker websites that share your information.** Not all brokers offer this option, but many do. Spokeo, one of the most popular sites, will remove your information within 48 hours of a request. **This list** at World Privacy Forum offers opt-out links to the biggest broker sites.
- **Adjust your privacy settings on social media accounts.** Review your settings on Facebook, Twitter, LinkedIn, Instagram, and Pinterest periodically, and make sure you're not sharing more than you want to.
- **Consider using an ad blocker.** An ad blocker is software that can be downloaded on your computer and is capable of removing online advertising and browser extensions.
- **Regularly clear cookies from your browser.** You may be wondering what a cookie is. A cookie, in technology terms, are small pieces of data that are used to identify your computer. To clear cookies from your browser, you can find this option in your computer's settings. Digital Trends, a tech website, offers instructions on how to disable cookies at **www.digitaltrends.com/computing/how-to-delete-cookies**
- **Do an Internet search on yourself, just to see what's out there.** If you find something you don't like, contact the site owner to see if they will remove it.[2]

[2] Howell, Elaine. "Don't Get Doxxed: Tell Data Brokers You're Opting Out". UCLA IT Services, Feb 23, 2017, www.it.ucla.edu/news/dont-get-doxxed-tell-data-brokers-youre-opting-out

Harassment Through Technology

Some people use technology—such as photos, videos, social media, and dating apps—to engage in harassing, unsolicited, or non-consensual interactions.[3] This is a very traumatizing and vulnerable position to be in.

The harassment can seem relentless and the offender uses the very devices that are vital to all of us to stay connected to our support systems to harm you. Not using technology or social media is often not a good option for victims of crime for many different reasons. However, enlisting the help of authorities can also be frustrating because filing criminal charges against someone requires proof of the offender's behavior. This proof is largely located on your personal devices. While most people react to harassment by immediately deleting the offensive content or messages, this in effect loses that "evidence" if criminal charges are to be filed.

This section will explain the different forms of online and technological harassment and gives suggestions for how to document this for any future or current legal reasons. Please know that at any point, an offender can escalate their behavior and become more violent especially when losing access they once had through harassment. Please meet with your advocate to develop a personal safety plan located at the end of this guide. Being prepared for any change in your situation will help you to both feel and be safer.

UNWANTED CALLS, TEXTS AND EMAILS

This type of harassment is by far the most common way offenders choose to harass their victims. It can be debilitating and frightening for a victim of crime to receive constant texts, phone calls, and emails that are at the least harassing and at the worst threatening and terrifying. Calls, texts, and emails from the offender can also be a violation of a protection order, if you have one in place.

The first thing many professionals will explain is that you want to make it clear you do not want any further contact with the offender, preferably in writing, and then cease contact with the offender. This means that as the harassment continues, do not respond to the offender unless you are telling them to stop contacting you. A documentation log to help you keep track of unwanted contact can be found in the Resources section of this guide. This log can help you document every instance of harassment and keep it organized. If you need to file a criminal complaint, it will show law enforcement the extent of the harassment in a logical and easy to follow format.

Taking screenshots of whole conversations and interactions with your offender is a way to document the harassment. Each device has a different way of taking screenshots. A screenshot is an image of the data displayed on the screen of a computer or mobile device. When capturing screenshots, make sure the screenshot captures the entire conversation even if it is in multiple photos, the date and time at the top of your phone, and the name of the other individual in the chat.

[3] "Using Technology to Hurt Others", Rape, Abuse & Incest National Network (RAINN), www.rainn.org/safe-tech

To learn how to take a screenshot on your device, you can do an online search or reference the chart to the right developed by the Safety Net Project at the National Network to End Domestic Violence from the series, "How to Gather Technology Abuse Evidence for Court".

Device	Take a screenshot	Find the screenshot
Windows laptop or computer	Find the key on the keyboard that says: PrtScn, Prt Scr, or Print Screen	Immediately after taking the screenshot, open a document that lets you paste an image (such as Word or Google Docs), and "paste" the screenshot.
Mac laptop or computer	At the same time, press these keys: Shift + Command + 3. This will save the screenshot onto your computer desktop.	Screenshot will be saved onto the desktop as a picture.
iPhone or iPad	At the same time, press the On/Off button + the Home button. For iPhone X, press the On/Off button + the Up Volume button.	Screenshot will be saved into your Photos app as a picture.
Android phone or tablet	Android devices differ. You should try the following options: 1) Down Volume button + Home button, 2) On/Off button + Home button. If neither of those work, try an online search for "How to take a screenshot on a [your specific phone or tablet]"	Screenshot will be saved into your Gallery as a picture.

SAFETY TIPS

- **Make it clear to the offender that you do not want further contact** of any kind then stop responding to the offender. Do not delete any messages. Take screenshots of text messages and missed calls. Print and save emails with the date and time received. If the calls go to voicemail and a message is left, do not delete them.
- **Many email services, including Gmail, have a place in which to report harassing emails.** Consider reporting if you feel safe to do so. Make sure to document any request of this nature and keep correspondence related to it. Remember to not delete or forward these emails.
- **Print the harmful emails and keep them in a safe place.** Make sure that the copies have the date, time, name, and email address of the offender.
- **Consider applying for a protection order.** In Ohio, there are many different types of protection orders you can apply for. If you are currently the victim in a case in which the offender has been charged with a crime you may file in the criminal court. Or you can file within the civil courts which do not require criminal charges to be filed. We encourage you to speak with an advocate and/or an attorney to determine what would be best for you.
- **Document evidence.** Enter each instance in a log that you keep with you while referencing the date and time so it is easily found in your phone. Again, do not delete anything.
- **If the content is too large for screenshots, then take a video of the harassment.** Be sure to hold your camera steady as you document the information.
- **Another helpful tip is to print out the call records from your phone bill.** This should be easily accessible in your account online or the monthly bill statement. See the Resources section at the end of this information for a sample documentation log.
- If your computer or phone doesn't allow you to take a screenshot, then **take a photo of the computer, phone, or tablet screen with another camera.**

SPOOFING

When calls and texts go unanswered, an offender may begin using different phone numbers or email addresses to contact you. They may also use an app that "spoofs" their number or email address so you are unaware who the caller is. Spoofing means that by accessing a free or paid app on their phone, they can generate fake numbers to be associated with their phone making you think someone else is calling. Documenting spoof calls can be tricky, but here are a few tips:

SAFETY TIPS

- **Screenshot your call records and record phone calls,** if legal in your state (need to ask an attorney about this so it is Ohio specific). We encourage victims to speak with an attorney if they choose to record phone calls. This can connect the offender to the fake numbers.
- **If law enforcement is able to view the offender's phone**, they may be able to match up calls and texts by the date and time, see an app on the offender's phone, or even subpoena the offender's records to match up dates and times.
- **Additionally, if the offender speaks in similar words as other calls and texts** with their own number, mention something only the offender would know and/or gives any other indication of their identity while using the spoofed number, law enforcement may be able use that information.

UNAUTHORIZED USE OF PERSONAL IMAGES

The use of revealing or sexually explicit images without permission is a form of harassment known as "revenge porn" or non-consensual pornography. This form of harassment can be debilitating for a victim of crime and can destroy a victim's, and sometimes their families', lives. Many unauthorized photo postings include the name and address of the victim. Release of these images without consent can ruin someone's chance at employment and housing. If this is happening to you it is important to do what you can as quickly as you can to have the images removed from the internet. Before the images are removed, make sure to preserve reliable copies of the content as it existed before it was removed.[4]

The Cyber Civil Rights Initiative is a non-profit organization that offers assistance to victims of cyberbullying and cyber harassment through its crisis helpline. Their website, www.cybercivilrights.org, houses many resources and options for assistance to victims of this type of crime. This website also has a detailed guide to the removal of online images throughout search engines and social media sites at www.cybercivilrights.org/online-removal.

One way to have the legal ability to have personal images removed is to copyright your images. Without My Consent is a project stewarded by the Cyber Civil Rights Initiative. Without My Consent provides a detailed explanation how copyright law can be used to combat the non-consensual distribution of intimate images at www.withoutmyconsent.org/perch/resources/wmctakedownv1-0.pdf.

Another way to have your personal images removed is to utilize the policies of social media companies. Many companies will now voluntarily take down non-consensual pornography regardless of whether the victim owns the copyright.

In Ohio, there are criminal laws protecting people from the unauthorized use of images. Please contact law enforcement or your victim advocate for more information on reporting these types of crimes. While it may be helpful to seek further assistance through these resources, we have also included the link to www.copyright.gov.

[4] www.withoutmyconsent.org/perch/resources/wmctakedownv1-0.pdf

Cybersafety on Social Media

Social media are interactive websites and apps that enable users to create and share content or to participate in social networking.

Here are nine social media networks being used most frequently:


Facebook


Instagram


LinkedIn


Pinterest


Snapchat


TikTok


Twitter


WhatsApp

YouTube

Users post photos, comments, videos, and can conduct business on these platforms. It's fair to say that many of us use social media platforms on a regular basis whether personal or professional. So when an offender seeks to harass, stalk, and commit crimes via social media, it can make the victim feel extremely exposed. In this section of the guide we will be discussing privacy and security in these various formats while sharing some specific ways to document abuse.

SAFETY TIPS[5]

- **Review your privacy settings.** Privacy settings control who sees what you share.
- **Review your security settings.** This is where you can change your password, username, or email.
- **Use a password that is hard to guess** but easy for you to remember.
- If you have friends or followers you don't know, **try not to post very private things**.
- **Talk to your friends and family about their social media use.** Even though you might be very cautious, they may not be. Ask them to get your permission before they share anything about you.
- **Use 2-step verification or login approval** for additional security. This requires a second password or approval process to access your account.
- **When capturing screenshots,** make sure the screenshot captures the harassing image, the name of whoever posted it, and the caption under the picture.
- **If the content is too large for screenshots, then take a video of the harassment.** Be sure to hold your camera steady as you document the information.
- **Take screenshots and/or print the profile page of the offender.**
- If someone is harassing you on social media platforms, **make sure to document** if the offender reacted to any of your posts either through commenting or "liking" a post.
- **Download your information** from Facebook in your Settings under "Your Facebook Information"

[5] www.techsafetyapp.org/online-safety/social-media-privacy

Most social media sites have information on how to report and change privacy settings.

The National Network to End Domestic Violence's Technology Safety website at www.techsafety.org has extensive guides to download for both Facebook and Twitter.

SAFETY & PRIVACY ON FACEBOOK
www.techsafety.org/resources-survivor/facebook

SAFETY & PRIVACY ON TWITTER
www.techsafety.org/safety-privacy-on-twitter-a-guide-for-victims-of-harassment-and-abuse

PRIVACY AND SECURITY

- **Social media sites have many different opt-in and opt-out measures listed in your account settings.** Even if you have looked at your account settings in the past, the options can change and many of us do not keep up with those changes.
- As we discussed earlier in this guide, **geotagging and location settings can be a problem for many reasons.** Though many social media sites strip this information from your pictures before it posts, some do not. You may be able to change theses settings on these social media accounts to prevent the pictures you post being detected.
- It is also important to remember that even if you have your location disabled and your pictures protected, your friends may not. **Tagging you in pictures or even "checking in" to locations, even if you are not tagged, could cause the offender to track you at their locations.** For safety tips related to geotagging, please visit that section in this guide on **page 9**.
- Facebook, Instagram, Twitter, Reddit, and Imgur all strip this information from the photos before it is shared. **However, any photos you share via text, email or on sites like Flickr do not.** You are able to Google instructions for removing this data from your pictures based upon the type of phone you have.
- **Harassment though social media sites is a very common form of harassment and very difficult to manage.** Your first response may be to report a harassing post to the social media site for removal. If you are wishing to file a criminal complaint, the evidence of the harassment could be lost. Before you report harassment on a social media site print out copies of the posts or damaging conversation before it is deleted.
- **Social media sites have settings that you can access on your account that can be changed to enhance your privacy and security online.** Remember that privacy and security settings may be in two different places in your account settings.
- **Facebook, Instagram, and Twitter have options that allow you to access and download your data.** This can be very helpful to law enforcement and may retain information that has previously been deleted. Instructions for downloading your social media data can be found in account settings within that specific social media account.
- **It is important to find out before you report someone on a social media site if that person will be notified that you did so.** For example, if you screenshot a post on Snapchat, the other user will be notified that you did. If you are attempting to gather data from Snapchat, a solution may be to use another camera to take a picture of the computer, phone, or tablet screen so that the offender is not notified that you took a screenshot. If offenders are then notified of this step taken against them, then it may be necessary to implement your safety plan. Consider taking a picture of the post with another phone so that you can capture the evidence without tipping off the offender that you are doing so.

APPENDIX A

Technology Safety Plan: A Guide for Survivors and Advocates

Technology Safety Planning with Survivors

Tips to discuss if someone you know is in danger

Technology can be very helpful to victims of domestic violence, sexual violence, and stalking, however it is important to also consider how technology might be misused.

1. **Trust your instincts.** If you suspect the abusive person knows too much, it is possible that your phone, computer, email, driving or other activities are being monitored. Abusers, stalkers and perpetrators can act in incredibly persistent and creative ways to maintain power and control.

2. **Plan for safety.** Navigating violence, abuse, and stalking is very difficult and dangerous. Advocates at the National Domestic Violence Hotline have been trained on technology issues, and can discuss options and help you in your safety planning. Local domestic violence and rape crisis hotline advocates can also help you plan for safety.

3. **Take precautions if you have a "techy" abuser.** If computers and technology are a profession or a hobby for the abuser/stalker, trust your instincts. If you think he/she may be monitoring or tracking you, talk to hotline advocates or the police.

4. **Use a safer computer.** If anyone abusive has access to your computer, he/she might be monitoring your computer activities. Try to use a safer computer when you look for help, a new place to live, etc. It may be safer to use a computer at a public library, community center, or Internet café.

5. **Create new email or IM accounts.** If you suspect that anyone abusive can access your email or instant messaging (IM), consider creating additional email/IM accounts on a safer computer. Do not create or check this new email/IM from a computer the abuser could access, in case it is monitored. Look for free web-based email accounts, and strongly consider using non-identifying name & account information. (example: bluecat@email.com and not YourRealName@email.com)

6. **Check your cell phone settings.** If you are using a cell phone provided by the abusive person, consider turning it off when not in use. Also many phones let you to "lock" the keys so a phone won't automatically answer or call if it is bumped. When on, check the phone settings; if your phone has an optional location service, you may want to switch the location feature off/on via phone settings or by turning your phone on and off.

7. **Change passwords & pin numbers.** Some abusers use victim's email and other accounts to impersonate and cause harm. If anyone abusive knows or could guess your passwords, change them quickly and frequently. Think about any password protected accounts - online banking, voicemail, instant messaging, etc.

8. **Minimize use of cordless phones or baby monitors**. If you don't want others to overhear your conversations, turn baby monitors off when not in use and use a traditional corded phone for sensitive conversations.

4. **Use a donated or new cell phone**. When making or receiving private calls or arranging escape plans, try not to use a shared or family cell phone because cell phone billing records and phone logs might reveal your plans to an abuser. Contact your local hotline program to learn about donation programs that provide new cell phones and/or prepaid phone cards to victims of abuse and stalking.

5. **Ask about your records and data**. Many court systems and government agencies are publishing records to the Internet. Ask agencies how they protect or publish your records and request that court, government, post office and others seal or restrict access to your files to protect your safety.

6. **Get a private mailbox and don't give out your real address.** When asked by businesses, doctors, and others for your address, have a private mailbox address or a safer address to provide. Try to keep your true residential address out of databases.

7. **Search for your name on the Internet.** Major search engines such as "Google" or "Yahoo" may have links to your contact information. Search for your name in quotation marks: "Full Name". Check phone directory pages because unlisted numbers might be listed if you gave your number to anyone.

Call the U.S. National Domestic Violence Hotline 800-799-7233 or TTY 800-787-3224

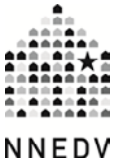
National Sexual Assault Hotline 800-656-4673 (RAINN) directly connects you to a local U.S. rape crisis program near your phone number.

Technology Safety Planning with Survivors: Tips to discuss if someone you know is in danger [Revised 2008]

Web: nnedv.org/safetynet • Email: SafetyNet [at] nnedv.org • Phone: 202-543-5566

APPENDIX B

Documentation Log



Sample Technology Abuse Log

Information About the Abuser	
Name of the person abusing or stalking you.	
Relationship of that person to you (if relevant).	
Contact information of that person	
Home address	Work address
Phone number(s)	Email address(es)
Online account(s), including screen name & type of online account (facebook, etc.)	
Other information about the abuser (that might be relevant)	
Description of the Abuse	
Date:	Time:
Describe the event:	
Type of technology involved:	
Were there any witnesses? What are their names?	
Documentation	
If you were able to document the abuse, what type of documentation do you have?	
Other Information	
Did you report it to the police? If so, what is the report number and officer name?	
Did you go to the hospital/see a doctor? If so, what was the hospital/doctor name?	

Additional Resources

Cyber Civil Rights Initiative (CCRI)
www.cybercivilrights.org

CCRI Crisis Helpline—844-878-CCRI (2274)

Women Against Cyberrape (WAC)
www.womenagainstcyberrape.com

U.S. Copright Office
www.copyright.gov

Heartmob
www.iheartmob.org

HeartMob is a platform that provides real-time support to individuals experiencing online harassment and empowers bystanders to act.

National Network to End Domestic Violence—Technology Safety
www.techsafety.org

This website is dedicated to helping survivors stay safe online and it is updated frequently. Under the Resources tab, there is a Survivor Toolkit to help victims navigate safety with technology. www.techsafety.org/resources-survivors

Information from Norton on VPNs
https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

The Ultimate Guide On How To Manage Social Media Privacy Settings, Jimit Bagadiya
www.socialpilot.co/blog/ultimate-guide-manage-social-media-privacy-settings

Stay Safe Online, powered by the National Cyber Security Alliance
www.staysafeonline.org

Has safety tips technological and online safety

US Department of Homeland Security Cyber Infrastructure (CISA Publications)
www.us-cert.gov/ncas/tips

Shares information and tips that describe and offer advice about common security issues for non-technical computer users including, but not limited to: Threats, Email and Communication, General Information, General Security Information, Mobile Devices, Privacy, Safe Browsing, Software and Applications

Women's Law.org (National Network to End Domestic Violence)
www.womenslaw.org/about-abuse

The email hotline will provide legal information to anyone who reaches out with legal questions or concerns regarding domestic violence, sexual violence, or any other topic covered on www.WomensLaw.org. This website has a comprehensive list of how-to guides and information about technological and online safety.

Glossary

Ad Blocker
Ad blocking or ad filtering is a software capability for removing or altering online advertising in a web browser or application.

Apps
A common term for “application”, a computer program or software designed to run on a mobile device such as a phone, tablet, or watch.

Browser
A software application for accessing information on the World Wide Web. When a user requests a web page from a particular website, the web browser retrieves the necessary content from a web server and then displays the page on the user’s device.

Cookies
Also called a HTTP cookie is a small piece of data sent from a website and stored on the user’s computer by the user’s web browser while the user is browsing.

Cyber Crimes
A computer-oriented crime is a crime that involves a computer and a network. The computer may be used in the commission of the crime or it may be the target. Examples of cyber crimes are fraud, trafficking in child pornography and intellectual property, stealing identities, or violation privacy.

Cyber Stalking
The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.

Cyber Harrassment
Also known as cyber bullying. The use of email, instant messaging, and derogatory websites to bully or otherwise harass an individual or group through personal attacks.

Cybersafety
Safe practices when using the internet to prevent personal attacks or criminal activity. The act of maximizing a user’s awareness of personal safety and security risks to private information and property associated with using the internet, and the self-protection from computer crime. Also known as online safety or E-safety.

Data
Facts, figures, or information that’s stored in or used by a computer.

Data Brokers
A company which specializes in collecting information about individuals from public records and private sources, including census and change of address records, motor vehicle and driving records, user-contributed material to social networking sites, media and court reports, voter registration lists, consumer purchase histories, most-wanted lists and terrorist watch lists, bank transaction records, healthcare authorities, and web browsing histories.

Doxxing
To search for and publish private or identifying information about a particular individual on the internet, typically with malicious intent.

Facebook
A popular free social networking website that allows registered users to create profile, update photos and video, send messages and keep in touch with friends, family and colleagues.

Flickr
An image hosting and video hosting service as well as an online community.

Geotagging
The process of adding geographical identification metadata to various media such as photographs, videos, text messages, QR codes, or RSS feeds.

Google
A company known for being an internet search engine and host of computer apps like Gmail, Picasa, and Google Drive.

Global Positioning System (GPS)
A navigational system using satellite signals to fix the location of a radio receiver on or above Earth's surface.

GPS Tracking Unit
A navigation device normally carried by a moving vehicle, person, or animal that uses the Global Positioning Unit (GPS) to track the device's movements and determine its location.

Imgur
Online image sharing community and image host. The service has been popular with hosting viral images and memes, particularly those on Reddit.

Instagram
A photo and video-sharing social networking service owned by Facebook, Inc. Instagram allows users to edit and upload photos and short videos through a mobile app.

IP Address
An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the internet. An IP address serves two functions: host or network interface identification and location addressing.

LinkedIn
A social network that focuses on professional networking and career development.

Location History
A cell phone feature found within a user's Google account that keeps track of all the places you visited throughout the day, every day.

Mobile Phone Tracking
A process for identifying the location of a mobile phone, whether stationary or moving.

Non-Consensual Pornography
Refers to the distribution of sexual or pornographic images of individuals without their consent. This may include images taken without consent or images taken with consent but later distributed without the consent of those within the images. These images are sometimes referred to as “Revenge Porn”.

Opt Out
To choose not to participate in or carry on with something.

Pinterest
An image sharing and social media service designed to enable saving and discovery of information on the World Wide Web using images in the form of pinboards.

Protection Order
An order issued by a court to protect a person, business, company, establishment, or entity and the general public, in a situation involving alleged domestic violence, child abuse, assault, harassment, stalking, or sexual assault.

Reddit
A social news aggregation, web content rating, and discussion website. Registered members submit content to the site such as links, text posts, and images which are then voted on by other members.

Screenshot
Also known as a screen capture or screen grab, is a digital image that shows the contents of a computer on display. A screenshot may also be created by taking a photo of the screen.

Security Program
Also known as cybersecurity software is any computer program designed to enhance information security.

Snapchat
A multimedia messaging app where pictures and messages are usually available for a short time before they become inaccessible to their recipients.

Social Media
Websites and applications that enable users to create and share content or to participate in social networking.

Spoofing
The act of disguising communication from an unknown source as being from a known, trusted source. A spoofing attack is a situation in which a person or program successfully identifies another by falsifying data, to gain illegitimate advantage.

Tracking App
An app that has a built-in function that can track not just the phone’s location, but other data found in the targeted device as well. This type of software is generally referred to as a cell phone spy all and there are many on the market today.

Twitter
A microblogging and social networking service on which users post and interact with messages known as “tweets”.

Virtual Private Network (VPN)
A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

OVWA is a private, non-profit organization.
Tax-deductible contributions are appreciated.

Contact us or visit our website at www.ovwa.org
to learn more about our services.

90 Northwoods Blvd., B-6
Columbus, OH 43235

phone 614-787-9000
fax 614-396-8863
info@ovwa.org

www.ovwa.org

This guide was supported by grant number 2021-VOCA-134145796 awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice through the Ohio Attorney General's Office. Victims of federal crimes will be served.