DOCUMENTATION TIPS FOR SURVIVORS OF TECHNOLOGY ABUSE AND STALKING

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of January 2025.

Perpetrators will often misuse technology to further abuse and control their victims. Misuse of technology could include monitoring technology use (including computers or smartphones), sending multiple unwanted or threatening text messages or voicemail messages, or posting negative comments or images of the survivor online.

In some cases, how technology is misused to harass and control may seem unbelievable. However, it is important to trust your instincts. If you believe that you are being monitored or stalked via technology, you might be. Narrowing down what is happening, including the tactic and the technology used, can help to determine if stalking is occurring, and if so, how to address it.

The first step is to document everything that is happening. Documentation is important for many reasons:

- It will give you a record of what is happening, which may be helpful if you want to pursue legal action.
- It will also alert you to any escalation in monitoring and control, which may indicate that the danger is increasing as well.
- It will help you see patterns of the technology abuse and may help determine how the abuser is misusing a particular technology.

Documenting Tips

Keep a log of all incidents, even if you are not sure if you want to involve the police. Some of the information you might want to record is the date, time, location, officer information (if reported), witnesses (if any), suspected technology involved (e.g., phone, email, etc.) and a brief description of what the abuser did.

Save everything related to the event or incident. If you receive a threatening note or a threatening message by email, text message, or voicemail, make sure you save it. Take a photo or screenshot of the message. While it may be tempting to delete it, saving it could show patterns to help you determine safety strategies and provide the needed evidence.

Think about the technology that you suspect the abuser could be using. In some cases, survivors have strong suspicions about what technology the abuser is using based on the type of abuse, the tactics involved, and what they know about the abuser.

Think about your safety first. In some cases, when abusers know that victims are documenting the abuse they might escalate their monitoring, control, or physical violence. You will know best how to assess the situation and what could happen. Trust your instincts and do what is safest for you.

Document only relevant information. Keep in mind that this information could potentially be introduced as evidence or inadvertently shared with the abuser at a future time. For example, you may not want to document personal photos that aren't being used as part of the abusive tactic.

What to Document

Emails

- Emails contain IP addresses, which could reveal the originating IP address and therefore the identity of the sender. Because of this, it's important not to delete the email and not to forward the email to someone else (as this action could cause you to lose the IP address).
- If saving email content by printing or taking screenshots, be sure to also save the email header (often hidden and can be found in the settings), which is where the IP information is stored. Depending on the email platform you are using (Gmail, Outlook, Yahoo! Mail, etc.), how you access the email header will be different. You can easily google this from a safe computer.
- If you're concerned that the abuser could access the account and delete emails, then try to print out or take screenshots of the content, including the headers. Forwarded emails will lose the identifying information needed for evidence.

Text Messages

- Text messages that are just stored on a phone may be inadvertently deleted or may be automatically deleted if you run out of space. Take a screenshot or a photo of the text messages with another device to retain the evidence.
- Also take a screenshot of the contact page to show that the harassing messages from the abuser are associated with the abuser's phone number.
- Text message content is kept by the mobile carrier only for a limited time. If you are working with the police, be sure to ask them to send a preservation letter to the telco as soon as possible, so the telco knows not to destroy the data.

Social Media/Internet Harassment

- To document evidence of harassment on social media, take a screenshot of the harassment/abuse on your computer or device.
- Some sites offer alternative ways to document activity on the site or on your page. For example, using Facebook's "Download Your Information" (DYI) feature, you can capture all content and save for later.
- If working with the police, they could send a letter to the social media or website company and ask them to preserve the account information and to not delete it.
- You may consider reporting the harassment to the social media or website company. If it violates the site's terms of service or content guidelines, they may remove the content. However, be sure that you document the abuse first if you want evidence of it.

Harassing Phone Calls

- You could consider recording your phone conversations to keep evidence of harassing or threatening calls. Check these legal guides[1] to see the laws relating to surveillance and listening devices for your state.

Phone Number/Caller ID Impersonation

- Document your call logs by taking a photograph of the Caller ID. Be sure to include the date and time of the calls.
- Keep your phone records to show the number of the originating call, date, and time.

Report to Police

- Document the time, date, and name of the assisting officer of any reports you make to the police and always ask for an incident report number (which you should also record as well).

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.

[1] https://techsafety.org.au/resources/legal-guides/