NNEDV

Assessing for Technology Misuse and Privacy Concerns with Sexual Assault Survivors

Technology tools have become woven into the fabric of our daily lives, and unfortunately sexual assault is no exception. Offenders misuse technology in order to commit, and cover up, sexual assault. In addition, the vast amount of information available online can compromise survivors' privacy. However, the digital trail left by that misuse of technology can be used by survivors and those who work with them to hold offenders accountable and online spaces can support survivors healing.

This handout includes information that advocates and other professionals working with survivors of sexual assault may use to help narrow down the possible technology that could be involved in the case, to gauge the survivor's knowledge and understanding, and identify where they might want assistance in navigating technology options.

Remember that our work begins by listening to a survivor's story and concerns. The needs and priorities of a survivor in the recent aftermath of an assault will differ from those of a survivor who was assaulted or abused many years or decades ago. Each survivor will use different language to describe their experience, and the person who harmed them. While the term, "offender" is used in this document, remember to use whatever language the survivor uses.

These questions are meant as a starting point for your work with survivors. This list is not intended as an intake form or required set of topics. Choose and adapt these topics as they seem relevant to your work together over the course of time.

1. Are you concerned about being harmed in person?
    - Do you think this person might be tracking your location?
    - Do you feel like there are places you can't go because the person will be there, or will be able to monitor you through video, audio, or through other people?
2. Are you concerned that your conversations are being monitored?
    - Does this person ever have access to your devices or accounts? Have they had access in the past?

- Where are you connected directly to this person online? Where are you connected through friends or other people?

3. Are you concerned about images, information, or rumors that might be spread about you through social media, email or a website to people you know?
    - Does this person have access to any place where information about you is stored, such as databases of school, employment, health or benefits records?
4. Are you concerned about the offender impersonating you online, or through texts, message or chat?
5. Are you concerned about your ability to continue using technology while maintaining your privacy?
    - Are there specific mobile devices or other technology that you want to go through to ensure that they are safe and secure?
    - Do you want to go through your social network accounts to figure out privacy and security settings?
    - Would you like to plan around "triggers" or stories in the news or social media that might be upsetting?
6. Are you concerned about information that is available about you on the Internet that could be used to harm you, for example your full name, address, school, or workplace?
7. Are you interested in more information about ways of talking to other people about the assault, including making a report?
    - Would you like to talk through concerns about speaking out online?
    - Would you like to learn more about reporting apps, anonymous reporting, or other ways to store information about the assault?
8. Are you concerned that online information like police reports, sex offender registries, news stories, or blog posts about you, the assault, or the offender might violate your privacy?
9. Do you have other concerns about your privacy or safety?

As you work with the survivor, here are some specific types of technology to keep in mind:

- Social media sites and apps, including posts, comments, pictures, video, live

video, location
- Online forums or email groups that both the offender and the survivor might belong to, for example at school or work
- Webcams on computers and mobile devices
- Dating and hookup sites and apps
- Online gaming, virtual reality and augmented reality apps and sites
- Location tracking devices, as well as location features on social media and mobile devices
- "Smart" and "connected" devices, part of the Internet of Things (IoT) that connect everyday devices to the Internet
- Assistive technology used by people with disabilities
- Account information from billing records, social media
- Databases and security cameras from places the offender has access to (businesses, schools, housing, workplaces, health care facilities, etc.)

Remember to factor in "old school" technology such as landlines, especially older cordless phones, or baby monitors. Older devices often offer less security, or have software systems that are no longer updated with security patches.

Also consider "social engineering," or manipulating our basic human desire to help others, can pose a risk to survivors' privacy and safety. The most secure technology systems can be compromised by third parties used to get information about a survivor.

Supported by US DOJ-OVC Grant# 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update out materials frequently. Please visit TechSafety.org for the latest version of this and other materials. For survivors experiencing sexual assault within the context of domestic, or intimate partner violence, we encourage advocates and survivors to consult the wealth of resources at TechSafety.org.