Tech Resources for DA Victims

Technology and the Internet are powerful tools for anyone experiencing domestic violence. They can be essential resources to access help and information, and valuable platforms to connect with friends, family members, advocates, and service providers. Unfortunately, they can also be used by abusive partners to begin, continue, or escalate abuse, making it all the more important to ensure your safety online.

Remember:

- Your computer and cell phone use can be monitored without you knowing it.
  - Computers store information about the websites you visit. That means bills you pay and purchases you make are tracked, and messages or emails can be retrieved. You should always consider that a computer might be monitored when you use it and be careful with what you send others or post.
- Your history can never be completely erased from a computer or device, even if you browse in "private" or "incognito" mode.
  - Safe computers can be found at your local library, Internet cafe, shelter, workplace, or computer technology center; avoid using a computer shared with him when researching things like travel plans, housing options, legal issues, and safety plans.
  - Your "browser history" is different than "cookies." Cookies allow marketers to track you; your browser history allows your abuser to track you.
- Email can be intercepted like physical mail.

  - Email can be a useful way to keep in touch with trusted friends and family members who may be aware of your situation. An abusive partner is likely to know this and may have access to your email account without your knowledge. To be safe, open an account your partner doesn't know about on a safe computer and use that email for safety planning and sensitive communications.
  - Be sure to sign out of your email and other accounts when you are done using them, so he doesn't have easy access to your communications.
  - Use several different methods of communication when contacting people so that you'll know if they tried to reach you elsewhere, and keep your monitored account active with non-critical emails in order to maintain appearances.
- Global Positioning System (GPS) trackers can be placed in your car or on items like your purse or cell phone.

What to do first?

1. Change your iCloud password.
2. Set auto-lock on your phone with a PIN or password he won't guess.
3. Create a new email account, without his knowledge.
   a. You can use Gmail, but ProtonMail and Tutanota are secure email providers with free plans. Using one of those might throw him off.

Tech Resources for DA Victims

4. Install a messaging app called Telegram on your phone in order to communicate with your counselor.
    a. When you send a message, make sure you use the "Secret Chat" feature as that will automatically delete your messages.
    b. Be careful about using WhatsApp instead. Many spy apps can read WhatsApp messages.
5. Do not use any computer or device to communicate with your counselor that he has access to. Work to clean your phone up, and keep him from accessing it. Use it exclusively for communications to your counselor/advocate/lawyer/shelter.
6. If you're sure he's tracking you via your phone AND you can't find the spy app, consider one of these options:
    a. Reset your phone to defaults.
    b. Consider purchasing a pay-as-you-go phone and keep it in a safe place for private calls. Use a password on your phone and update it regularly.
    c. Consider taking it into a cell phone service center to check for any spyware that may be downloaded.
    d. Do NOT restore your phone's apps from the cloud, because you will just restore the spy app. Manually go to the App Store and install them. It's a pain, but that is the only way to know you've gotten rid of the spyware.
7. If he is technologically savvy, be careful about connecting to wifi at home. Potentially, he could track when you go on the web and see you visit lawyer websites, apartment sites, shelters, etc.
8. Don't talk around an Amazon Alexa device. Your conversations can be recorded and tracked.

How to determine if you are being tracked?

1. Check your bill for extra large data usage
2. Has he had access to your phone in order to install a spy app, or does he know your iCloud password?
3. Have any odd messages popped up on your phone screen?
4. Does your battery seem to be draining quickly?
5. Does your phone sometimes turn on for no reason?
6. Are other apps running slower than normal?
7. Does it take forever to shut down?
8. Are there unfamiliar apps running in the background?
9. Does the screen stay on when you try to turn it off?
10. Look in the Applications list. Search for apps with names like "<something>spy" or *Service*.
11. Check the Permissions of all apps. Permissions include "Call logs", "Microphone", "Location", "SMS". Try to find any apps that have all these permissions, and then determine if they're suspicious.
    a. On Android, it is in Settings – Privacy – Permission manager.

Tech Resources for DA Victims

12. Does he know things about you – things you've said/emailed/messaged – that he shouldn't have known?

Potential Spy Apps

- Spyic
- Cocospy
- Glympse
- mSpy
- Mobistealth
- Flexispy
- Highster Mobile
- Minspy
- Flexispy
- Anything with a name of *Spy*

Passwords

- The length of a password is more important than it's complexity. Consider using the name of a favorite song; don't use your kids' names or birthdates or something he could guess. Try to use a password that is at least 10 characters long.
- Use passwords that are unique to each site. Don't reuse the password, for instance, you use for banking to be your email password also.
- Try not to write down your passwords, especially in a place he could find. Assume he is going through your belongings when you are not there and that he is snooping around. He may get suspicious and that will increase the intensity of his searches.

General Cybersecurity Guidelines

- Don't click on a link in an email or text unless it is from a source you trust AND you are expecting it. It's better to search for the website on Google or type in the link yourself in a web browser.
- Don't open any email or message attachments unless it is from a source you trust AND you are expecting the file.
- Make sure you stay current with software updates for all your devices and apps.
- Use strong passwords that are unique to each account/site you use.
- Use multi-factor authentication (MFA) if you can.
- Never give out your password over the phone.
- Posts on social media are never truly private, no matter your settings: once it's online, it's no longer under your control. Be protective of your personal information and remember that phone numbers, addresses, handles, and personal details (like birth date, schools you attended, employers, and photos with landmarks) may make it easier for someone to reach you.
- Set boundaries and limits, and ask people not to post personal information, photos, or check-ins you aren't comfortable with. Check your social media settings to make sure your privacy settings are strict, and disable the ability for other people to tag you in their photos or posts. Similarly, don't post information about people without their consent – you could jeopardize their safety or the safety of others.
- Other common apps can also be used to track you. Find My Phone, Facebook, Instagram, and Snapchat all have functions that may help someone track you.

Tech Resources for DA Victims

Helpful Apps

Here is a list of potentially useful apps, from recording conversations and phone calls to keeping a log of abusive incidents to how to recognize an abuser.

- Rev Voice Recorder and Memos (or any Voice Recorder app)
- TapeaCall Pro
- VictimsVoice PWA
- Noonlight
- MyPlan
- RUSafe
- DocuSAFE Evidence Collection