# TECHNOLOGY SAFETY PLANNING WITH SURVIVORS

Technology can be very helpful for survivors of interpersonal violence by connecting people with resources and support networks. However, it is also important to consider when technology may be misused and have strategies for what to do if you feel your technology use is being monitored.

1. **Trust your instincts.** If you suspect the abusive person knows too much, it is possible they are monitoring your digital presence.
2. **Take precautions if you have a "techy" abuser,** especially if computers or technology are a profession or hobby for the abuser.
3. **Change passwords, security questions, and pin numbers frequently.** Think about anything that requires a password: banking, email, social media, etc.
4. **Create new email or IM accounts.** If you suspect that an abusive person has access to your email or instant messaging, consider creating new accounts *from a safer computer or phone.* Do not create new accounts from a computer the abuser could access. Use non-identifying name and account information (not YourRealName@email.com). Deleting accounts that the abusive person may be monitoring might result in them suspecting a new account.
5. **Keep personal information private.** Be cautious of what info is available to employers and colleagues. And, if you give out personal info when signing up for deals or services, it could be sold to a publicly accessible database.
6. **Use a safer computer or cell phone.** If anyone abusive has access to your computer or phone, they might be monitoring you. Phone logs or billing records could reveal plans to an abuser. Try to use a safer computer/phone when you look for help, a new place to live, banking, etc. It may be safer to use a friend's device, or use a computer at a public library, community center, or your workplace, or use a donated or prepaid phone.
7. **Turn off GPS on all electronic devices (cell phones, digital cameras, laptops, etc.).** Follow user manual instructions. And consider turning off GPS for family members and children too.
8. **Talk to family and friends about tech safety needs.** Ask your friends/family not to post pictures, comments, or other information that may allude to your location or other personal information.
9. **Be cautious of Spyware.** Spyware programs can be hard to detect, downloaded onto a computer/phone quickly, and allow someone to track everything on a cell or computer. Some spyware can allow abusers to turn on webcams, take screenshots, etc. Clues that spyware may be on your device are:

- Physical access to the phone by an abusive person or someone they know. Most phone Spyware requires someone downloading it.
- If an abusive person knows more than they should about information in digital communications.
- Strange activity on the phone/computer, such as increased battery or data usage, the phone shutting down, or dropped calls. Note: Some spyware won't cause any operation or function changes in a device.

If you think your computer or phone has spyware, keep using it for simple things others already know about you. For searches related to safety, use a safer computer or phone. To remove Spyware from a phone, try resetting it to factory settings. Removing spyware from a computer is extremely difficult, and Spyware can be transferred with files to a new device. If you need access to a file on a new device, it's best to put that file in a cloud-based location.

10. **Be cautious of cordless phones and baby monitors.** Abusers can use these to overhear conversations and plans.