Tech Safety Plan – These are some general guidelines. There is specific information in some of the other documents. If you have any further questions, don't hesitate to contact COPE for help. The website GoAskRose.com is also a good source of info, as well as TechSafety.org.

1. On the computer (Even if you only use a SmartPhone, read through this, because you will need to do some of this on your phone instead):
    a. Clear browsing history after each use OR use Incognito Mode. Erase History is usually accessed in the upper right corner – look for "settings".
        i. Microsoft Edge: Upper right...>settings>Clear Browsing Date>Choose what to clear
        ii. Chrome: Upper right...>settings>advanced settings>clear browsing data.
        iii. Microsoft Explorer: Look in the upper right corner on the toolbar for a gear>safety>delete browsing history.
        iv. Firefox: Hamburger>options>Privacy & Security (on the left menu)>scroll down to History. On the right will be a button to clear history.
        v. Remember, HELP is your friend.
        vi. Opera: Everything is on the left. Click the red O>History>Clear browsing data
        vii. Safari: In the Safari app on your Mac, choose History > Clear History, then click the pop-up menu. Choose how far back you want your browsing history cleared.
        viii. If your abuser still has access to your computer, then after you clear your history, go back and go to some "safe" sites, such as a shopping site or news site, so that they don't become suspicious.

    b. Use a private or incognito window – usually accessed via the upper right corner.
    c. If you use Google, it will prompt you to sign into your account wherever you are. If you don't have to, don't. Don't sign into things using Facebook, either.
    d. Create a secret email account. Outlook is the only one that doesn't require a phone number.
    e. Social Media – lock down privacy, friends lists, and uninstall unknown apps on FB. Instructions: https://qz.com/1233344/how-to-delete-apps-harvesting-your-data-on-facebook-and-how-to-delete-your-facebook-account/
    f. Create decoy accounts –
        i. Fake social media accounts
        ii. Create a fake business for a fake job
        iii. Create fake SEO (Change the google results to things you've written about yourself)
    g. People searches – remove your info from public sites and databases.
    h. At home, check your network/router for unauthorized devices.
    i. Don't commit crimes. There are public records of crimes.
    j. Teach your children about privacy online.
    k. Check computer for viruses/malware/keystroke loggers. Use an anti-keylogger software, not just antivirus.
    l. Delete stored passwords and use a password manager. Enable 2FA (two factor authorization or authentication/2 step verification.)
    m. Password trick: use Leet speak – use symbols for letters. Example: Instead of using "Robert" as a password, use "R0b3rt" (The letter "o" is actually a zero.)
    n. "Wipe" your computer – reinstall your operating system.
    o.

    REMEMBER – if you don't know how to do something, you can always use the HELP button, or google it. For example, "How do I erase my history on Microsoft Explorer?"

2. Freeze your credit

3. Phone safety
    a. Get a "burner" phone OR use phone in incognito mode.

b. Do not use Facebook messenger on your phone if possible. Check DM's on a safe computer, such as at the library.
c. Once you're away from your abuser or when you can do so without fear of repercussions, reset your phone to factory settings.
d. Look for spy apps or reload system to remove spy apps.
e. Install secure texting app on your phone such as Telegram.
f. Keep location services turned off unless you absolutely need it.
g. Install a panic button such as Noonlight (see additional handout)

This is an example of what a keystroke logger looks like.