

Are you being stalked or watched?

TECHNOLOGY CAN MAKE IT EASIER TO STALK SOMEONE. If you suspect that you are being monitored, **IDENTIFY PATTERNS** - does your stalker know who you've been talking to on the phone, know what you wrote in an email, show up where you go, or know where you were last night after a Facebook post? Have you been getting a lot of strange emails, phone calls, or text messages?

REMEMBER: Making some safety changes may also alert a stalker that you are taking steps to improve your privacy and possibly increase your risk. You can contact your local domestic violence/sexual assault service provider for safety planning assistance.

Consider some of these tips to protect yourself from being monitored using technology:

ACCOUNT PASSWORDS



Change all passwords and security questions. Use phrases rather than words. Use symbols and numbers. Do not use your name, birthday, child's name, pet name, or any information your abuser can easily guess.

CELL PHONES



Turn off Location Services when not in use. Most phones can tell others exactly where you are. Go to **Settings** -> **Location Services**: set "off" for ALL applications.

Turn off Bluetooth when not in use.

Contact your Service Provider – find out if there are any unknown applications running on your phone. Ask to include a pass phrase to access your account over the phone. Tell them to NEVER share your location or information.

Consider purchasing a new phone, additional phone, or use Google Voice.

COMPUTERS



Use a safer computer – a friend's, the library, or at work.


Install anti-virus software.

Do not share account information or passwords.

Be careful with what you post online. It will stay there forever, even if you delete it.

SOCIAL MEDIA



Review/edit account and privacy settings. Look for the  symbol.

Turn off Location Services (phone, tablet, and computer).

Don't post pictures. If you do, make the posts private. If location services are "on" on your device, all pictures will be geo-tagged with your exact location.

Tell your friends/family not to tag you, your kids, or post pictures of you.

EMAIL



Change passwords and/or accounts.

Log out when you are done.

Limit the information you send about your location, plans, or anything else your abuser could use to stalk you.

Never open attachments from unknown sources.

Tell friends and family not to share your info.

Save and/or print harassing emails as evidence.

AUTOMOBILE



Check your car for hidden tracking devices. Law enforcement or a trusted mechanic can search your car.

National Domestic Violence Hotline:

1-800-799-7233

National Sexual Assault Hotline:

1-800-656-4673

Maryland Statewide Helpline:

1-800-MD-HELPS

With all the technology we use, it is easy for people to stalk our activities without our knowing. If this is happening to you, there are safety options available.

PASSWORDS and USERNAMES: “Password” and “123456” are not the safest passwords. If you suspect someone unsafe knows your password, you can change it from a safer computer (i.e., a friend’s or at the library). Use symbols (@, \$, &, !), numbers, and some capital letters. Do not use your pet’s name, your child’s name, your birth date, address, or any other identifying information that anyone also knows or could easily guess. Answer security questions with false answers. You can use the same answer every time so it’s easier to remember (e.g., Mother’s maiden name? Answer: Besafe). Consider creating usernames that are unrelated to your actual name and are hard to guess. Do not store your usernames/passwords on your computer, in your cell phone, or in a notebook in your desk. These can all be found very easily and can give people access to all of your critical information.

CELL PHONES: If you think someone is monitoring you through your phone, you can get a new or second phone and number. You can get cheap phones that allow you to pay as you go. A Google Voice phone number is an independent number that can be directed to your cell, home, or office phones, or elsewhere (google.com/voice). You can also block people from calling you. Lock your phone with a safe passcode. Be suspicious of people calling from unknown numbers and with strange voices; people can use voice-changing technology to avoid being identified.

Location services and Bluetooth are on most phones and make it VERY easy to track your location and connect to your phone without your knowledge. For instance, when you take photos or make posts on social media and location services are “on,” people can see exactly where you are in and when you posted it. Go to “settings” and turn OFF both location services and Bluetooth. If you absolutely need location or Bluetooth services for an app, turn it on for only short times when needed. Delete unknown apps and ones you do not use. Call your cell phone provider and tell them not to tell anyone your location or other identifying information. Ask them to double check the location settings on your phone and make sure there are no “third-party” or unknown applications on your phone.

COMPUTERS: People can follow you by looking at the websites you have visited. You can use incognito or safe mode. You can choose to use a safer computer (a friend’s or one at the library) when doing Internet searches or anything that involves personal information. Install anti-virus or anti-spyware software on your computer (e.g. Avast is a free protection software). Without adequate protection, someone can put spyware on your computer and track every key that you hit. Use a safe password (see above) to unlock your computer and do not give anyone this information. Always lock or logout of your computer when you are done.

AUTOMOBILE: If someone is showing up unexpectedly wherever you drive, then it’s possible that he or she has put a tracking device in your car. These devices are very easy to buy and easy to hide on or in the car. Some devices can be dangerous and turn off your engine at your stalker’s desire, leaving you stranded or unable to control your car. You may decide to go to a trusted mechanic or law enforcement agency to have them search your car. If a device is found, have the inspection company write a report about what is found, the date of the inspection, and their company information. Take this documentation to the police. The GPS system in your car (if you have one) saves data about where you have been. If the person stalking you owns the car, he or she is able to get the location information from the police. The best options may be to have a technician remove the GPS system (which may be expensive) or use a different car (such as Zip Car).

EMAIL: Consider creating a new email account if you know someone is using email to harass or stalk you. You can have emails from your old account forwarded to your new account so you don’t miss anything. Create a new safe password. Always log out when you are done: just closing the page does not log you out. Do not tell anyone your log-in information and try not to share personal information in your email (e.g., where you are going, where you live, financial information, daily schedule etc.). Never open attachments from unknown sources. Watch out for “spoof” emails: individuals can send emails that look like they are coming from someone else or so your spam folder does not catch them. Save emails from the person harassing you—these can be used as evidence in the future.

SOCIAL MEDIA: Social media is everywhere; it’s fun and hard to quit. The problem is that it is very easy to find personal information about you through social media. If you do not want to delete your accounts, check your privacy settings and make everything “private,” visible to only your friends, or only you. If your friends can see the personal information, the stalker may be able to use your friends to get information about you. Be careful when you or others post pictures online. Landmarks in pictures make it easy to identify where you are, and pictures are also tagged with your exact geographic location if your location services are still enabled. Ask that people not tag you or your children in posts, pictures, or any social media. Be aware that online dating or hook-up sites ask for a lot of personal information; it is easy for people to create fake accounts to follow you or find out information about you.

