

TECH TOP 10 TIPS
- SOCIAL MEDIA USE BY SURVIVORS -

#1

Survivors should make strong passwords and NOT share those passwords WITH ANYONE! A mix of letters, numbers and characters makes stronger passwords, NOT personal information such as birth dates or pet names. Survivors should choose security back up questions so that no one could guess the answer.

#2

Friends of friends are a lot more people than one might think. If a survivor has 130 friends and each of those friends has 130 friends and each of their friends has 130 friends then **2.1 million** people have access to the survivor's Facebook page! A survivor should consider account settings that allow only confirmed friends to view personal information.

#3

Privacy settings are crucial. Privacy settings put in place by the social media provider – Facebook, Twitter, MySpace, LinkedIn – are not the most secure settings. Counsel survivors to regularly review those settings and adjust them. To learn more, review the specific site's privacy page, e.g., <http://www.facebook.com/policy.php>

#4

Even if a survivor does not use social media, talk to the survivor about whether children, family or friends do. A survivor's location or other confidential information could be revealed through those posts. Suggest that survivors discuss safety and confidentiality needs with their children, family and friends.

#5

Cell phones come with GPS tracking that makes it possible to pinpoint a person's location. Many SmartPhones use this technology for social media check-in sites like Foursquare (see <https://foursquare.com/about>). Survivors who need to maintain a confidential location should be aware and cautious of using these sites and may want to turn off the GPS function on their phones.

#6

Physical access to a computer or cell phone is not necessary to put spyware on these devices. It only takes a minute to install spyware, which enables a third party to have access to all of the information on a cellphone, computer or other device. Remind survivors to keep their devices password protected and with them at all times.

#7

Camera-ready cell phones and many modern digital cameras put location information into photos that can be used to pinpoint where the photo was taken. Counsel survivors about removing this location information before posting any photos on the Internet or social media site. Check out <http://www.switched.com/2011/01/24/keep-your-photos-exif-geotag-data-safe/>

#8

What survivors post or is posted about them may be used against them in a court of law – in custody, divorce, PFA, and any other civil or criminal cases.

#9

A picture is worth a thousand words. Technology now provides the ability for abusers to send emails and texts that will disappear after the survivor opens them. In order to preserve the evidence of these contacts, a survivor should photograph the email or text message with a digital or cell phone camera.

#10

Use a safer computer or cell phone. Spyware can be installed on a computer or cell phone without the survivor's knowledge. If an abuser mysteriously knows private details or recent activities, the survivor may want to limit computer or cell phone use. For privacy, a survivor could use a public computer at the library and/or obtain a cell phone from the domestic violence program through the Hopeline Program.