Social Networking Risks, Privacy and Safety Planning

RISKS

Abusers can use social networks to stalk, harass and gain information about victims
- Social networks do not show record of who looks at your page when, which parts of your page, for how long, etc., therefore someone could monitor your page without your knowledge.
- An abuser may impersonate the victim w/ new pages or by hijacking victim’s page.
- Can “friend” (Facebook & MySpace) victim’s friends and family and gain at least some level of access to personal information
- May be able to find victim’s profiles and/or other information through search engines.

GPS and other Location-Based Social Networking: programs that run through cell phones, on Facebook, etc. allow a person to “check-in” at locations; this reveals current location information to anyone connected w/ that person in their social network.
- Facebook Places: allows the owner of an account or a friend to check-in and give current location information; privacy settings can be customized to prevent this!
- Geotagging Photos: pictures taken on smartphones (iPhone, Droid, Blackberry, etc) may have location information automatically embedded in the data of the photo based on the phone’s GPS. Whether this information is displayed varies depending on which site it is posted. This can be turned off on all phones!

Spyware: can be installed on a computer either physically or remotely through an email, instant message or other download; this can give abusers information about passwords for social networks and other accounts

PRIVACY

*REMEMBER: NOTHING posted online through a social networking site or blog is going to be completely private. Therefore it is important to weigh the costs/ benefits when choosing where and how to use social networks.

That being said...privacy settings can be made more secure.

On Facebook:
You can set account security to notify you if a new computer or mobile device is used to log in to your account. You can also view recent account activity to ensure that you know where and when your account was last accessed.

How to do this: Log in to Facebook account, Click the far right tab: ‘Account’, select: ‘Account Settings’ from the drop-down menu. Scroll downscreen to ‘Account Security’ and click that. This will open the option for notification as well as information about the most recent login.

Applications and Games: To play a game or use an application you are asked whether you wish to “allow access” in order to play the game, use the application, take the quiz, etc. Allowing access allows the creator of the application access to your profile information. Friends’ information can also be pulled and accessed by the creator. So even if you don’t use applications, but your friends do, the creator of those games may be able to access your information.

To change these settings and deny access: Log in to account; select ‘Account’ on the far right of the screen. Select: ‘Privacy Settings’ from the drop-down menu. On the bottom left of the screen you will see ‘Applications and Websites’. Click: ‘Edit Your Settings’. By turning off ‘Platform Applications’ you can cancel access to creators of any applications you may previously have used, and this will prevent your information from being shared when friends use applications.

Public Search: A Facebook account may be searchable through Google, Bing, etc.

To shut this search option off: Log in to Facebook, Click: ‘Account’ on top right of screen, select: ‘Privacy Settings’ from drop down menu, select: ‘Edit Your Settings’ under ‘Applications and Websites’ at the bottom left of your screen. The last option in the list that appears is: ‘Public Search’. Click on the button to the right of that, which reads: ‘Edit Settings’. If the box next to ‘Enable Public Search’ is checked, then your account is search-(and find)-able. Click the box to un-check and disable public search.
Facebook Directory Search: Even if Public Search is disabled, an account may be searchable on Facebook’s directory.

To check the status of, and change, this setting: follow the above directions to the ‘Privacy Settings’ main page. At the top you will see: ‘Basic Directory Information’. Click ‘View Settings.’ This allows you to customize who can search for you on Facebook, and who can see what information.

Other Privacy settings on Facebook are customizable. From the ‘Privacy Settings’ page you can view current settings and customize who can view certain things, who can post on your page, etc. You can disable friends from being able to “check you in” under the Places Application, which reveals up-to-the-minute location information (people often use this application to check-in at restaurants, movies, etc.). You can also block certain people, customize groups, and learn more about Facebook’s privacy policies. You can also choose how much information is available by making choices of what you list in profile information; for example, it is not necessary to list employer, relationship status, interests, etc.

*KEEP IN MIND: with large “Friend” groups that most Facebook users have, it can still be a challenge to control what information about you is on FB!

Photos: anyone can post a photo, with you in it, and tag you in it- which means it will list your name under the photo for anyone else who views it. If a friend posts photos, and they don’t have album settings private, anyone may be able to view those. Any photos you are tagged in will be listed under ‘Photos of Me’ on your account. You can un-tag yourself in a photo, so your name won’t be attached to it anymore, but unless you posted the photo, you can’t remove it entirely.

SAFETY PLANNING

** Awareness is key- there may be more information “public” online about us than we would imagine. Try searching your name on Google, Bing, etc. and see what comes up!!

Some Tips:

- Google yourself
- On Facebook, periodically view “Photos of Me” to see what’s on there.
- Talk with friends and family about posting (or not posting) photos you may be in on facebook or other social networking sites.
- As Facebook grows and changes, the default privacy settings may change. It’s a good idea to 1. pay attention to news stories or updates from Facebook re: updates and changes to learn how that may affect privacy settings, and 2. periodically check your settings.
- Visit: www.icanstalku.com for valuable information about privacy settings around photos and how to disable Geotagging on smartphones.
- Talk to your kids about all internet use; including major social networking sites.
- Be thoughtful about what you’re posting, privacy settings, and whose “friendship” you accept/ who you connect with online.
- Set unique passwords & security questions.

If abuser is impersonating, harassing, monitoring, etc. victim online there are options for recourse:

- Reporting inappropriate or false content/ pages to site owner may result in removal of content or page if it violates terms of use.
- Most sites have process for users if account is compromised.
- Reporting to Law Enforcement: If an abuser is stalking, harassing or posting fake/ fraudulent information about you online always save/ print messages for documentation.
- Law Enforcement (LE) resource: www.search.org maintains an ISP contact list of the appropriate contact person at all social networking sites to begin/ assist an investigation.
- LE can send preservation letters to keep evidence from being deleted; subpeonas or warrants can be sent to collect identifying information of the user/poster (IP address, email address, time of logins, etc.).
- LE should always specifically request that information about any beginning or pending investigation is not given to the owner of the account
- Misuse of online spaces may be violation of PFA or could be included in application for PFA.

More information is also available from the National Network to End Domestic Violence (NNEDV) at: www.nnedv.org