Social Networking Privacy: How to be Safe, Secure and Social [1]

1. What information are you sharing when you use social networks?

The kinds of information that you may be sharing on a social network includes:

- **Your profile.** Most social networks allow users to create detailed online profiles and connect with other users in some way. This may involve users sharing information with other users, such as one’s gender, age, familial information, interests, educational background and employment.

- **Your status.** Most social networks also allow users to post status updates in order to communicate with other users quickly. Though there may be privacy settings to restrict access to status updates, these networks are frequently designed to broadcast information quickly and publicly.

- **Your location.** Many social networks are designed to broadcast your real-time location, either as public information or as an update viewable to authorized contacts. This might allow users to “check in” to a local event or business, or share one’s location with contacts within their network.

- **Shared content.** Many social networks encourage users to share content, such as music, photographs, videos and links to other webpages.

All of this sharing reveals information about you, including contextual information you may not even be aware of. By sharing this information online you may be providing enough information to allow advertisers to track you or hackers to take advantage of your online identity. Therefore it is important to be aware of the information that you are providing and to be conscious of the choices you can make to protect your privacy.

2. How may your social networking information be used and shared?

**Publicly available information.** Every social network allows you to post some information that is completely publicly accessible. This can be anything from your username to individual posts, to your entire account. These kind of “public” posts are not blocked behind any kind of access restriction. Anyone, including strangers, can view whatever is posted as “public.” However, there may be other data that you share publicly without realizing it, and there are less obvious ways that your information may be treated as public without your permission, including:

- Certain information may be publicly visible by default. In some situations, a user may be able to change the privacy settings to make the information “private” -- so that only approved users can view it. Other information must remain public; the user does not have an option to restrict access to it (frequently such information includes your account name).

- A social network can change its privacy policy at any time without a user’s permission. Content that was posted with restrictive privacy settings may become visible when a privacy policy is altered.

- Approved contacts (people on your “Friends list” or people that “follow” you) may copy and repost information – including photos or personal information – without a user’s permission, potentially bypassing privacy settings.

- Third-party applications that have been granted access may be able to view information that a user or a user’s contacts post privately.

- Social networks themselves do not necessarily guarantee the security of the information that has been uploaded to a profile, even when those posts are set to be private. While security flaws and breaches are usually quickly fixed, there is
Advertising. Your own publicly posted content isn’t the only way that you can be tracked, and advertisers are very interested in the information that can be gathered by tracking your online activity. This may include:

- Tracking which websites a user has viewed
- Storing information associated with specific websites (such as items in a shopping cart)
- Analyzing aggregated data for marketing purposes

Behavioral advertising is the term used to describe the practice of tailoring advertisements to an individual’s personal interests. Social networks that provide their services without user fees make a profit by selling advertising. This is often done through behavioral advertising, also known as targeting. This practice is appealing to marketers because targeted advertisements are more likely to result in a purchase by a viewer than comparable non-targeted advertisements. They are valuable to social networks as they can be sold at a higher price than regular ads.

Third-party applications are programs that interact with a social network without actually being part of that social network. These applications take many forms but some typical and popular forms include games that you may play with contacts, online polls or quizzes, or third party interfaces with the social network. To make these applications useful, social networks may allow developers automatic access to public information of users, and may even access some private information, when a user grants the application permission. You may inadvertently grant an application access to your profile without realizing the extent of the permissions being granted. Some facts to keep in mind when considering using third-party applications:

- They may not be covered by the social network’s privacy policy. Most social networks do not take responsibility for the third-party applications that interact with their sites
- They may not be guaranteed to be secure.
- They may gain access to more information than is necessary to perform their functions.
- They may contain malware designed to attack the user’s device.
- Third-party developers may report users’ actions back to the social networking platform.
- A social network may have agreements with certain websites and applications that allow them access to public information of all users of the social network.

Government and law enforcement officials can monitor social networks for valuable information. Law enforcement agencies can and do monitor social networks for illegal activity. During an investigation, law enforcement will often turn to a suspect’s social network profiles to glean any information that they can. Though each social network has adopted its own procedures for dealing with requests from law enforcement agencies, it’s important to keep in mind that the degree to which these sites cooperate, or don’t cooperate, with law enforcement may not be fully explained in the privacy policy.

Employment. Potential employers are generally permitted to use whatever information they can gather about an applicant in making a hiring decision. Although there are legal risks, including possible violation of antidiscrimination laws, employers are increasingly turning to social media to inform their decisions. It’s important to know what information can be seen by non-contacts and to consider what kind of conclusions might be drawn from it.

The Fair Credit Reporting Act (FCRA) sets limits on what information employers can get from background checks and how they can use that information. However, the FCRA only applies to employers using third-party screening companies. Information that an employer gathers independently, including from informal Internet searches, is not covered by the FCRA.

Employers frequently monitor what employees post on social networking sites. In fact, many companies have social media policies that limit what you can and cannot post on social networking sites about your employer, and hire third-party companies to monitor online employee activity for them. Some states have laws that prohibit employers from disciplining an employee based on off-duty activity on social networking sites, unless the activity can be shown to damage the company in some way. In general, posts that are work-related have the potential to cause the company damage. The National Labor Relations Board (NLRB) has issued a number of rulings and recommendations involving questions about employer social media policies. The NLRB has indicated that these cases are extremely fact-specific. It has provided the following general guidance, however:

- Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.
- An employee’s comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.

3. Privacy policies
Most people skip over the privacy policy when joining a social network. However, users can learn a lot of useful information by reviewing a privacy policy before signing up for service. A social network’s privacy policy will explain how the social network will collect and use information about people who visit the site.

When reviewing a privacy policy, remember:

- Privacy policies can change – sometimes dramatically-- after a user creates an account.
- Terms of service may have information just as important as the privacy policy, so always review those as well.
- The privacy policy only covers the social network. It does not, for example, cover third-party applications that interact with the website.


4. Tips

There are many ways that information on social networks can be used for purposes other than what the user intended. Any time you choose to engage with social networking sites, you are taking certain risks. However, these practical tips may help you minimize the risks of social networks.

When registering an account:

- Use a strong password different from the passwords you use to access other sites. Ideally, use a password manager to generate and store your passwords.
- If you are asked to provide security questions, use information that others would not know about you, or, even better, don't use accurate information at all. If you are using a password manager, record the false questions and answers and refer to your password manager if you need to recover your account.
- Consider creating a new email address to use only with our social media profile(s).
- Provide the minimum amount of personal information necessary, or that you feel comfortable providing.
- Review the privacy policy and terms of service.
- During the registration process, social networks often solicit you to provide an email account password so that they can access your address book. If you consider using this feature, make sure to read all terms so that you understand what will be done with this information.

General privacy tips for using social networks

- Become familiar with the privacy settings available on any social network you use, and review your privacy settings frequently. On Facebook, for example, you may want to make sure that your default privacy setting is "Friends Only". Alternatively, use the "Custom" setting and configure the setting to achieve maximum privacy.
- Be careful sharing your birthday, age, or place of birth. This information could be useful to identity thieves and to data mining companies. If you do consider posting your birthday, age or place of birth, restrict who has access to this information using the site’s privacy settings.
- Try to stay aware of changes to a social network’s terms of service and privacy policy. Consider subscribing to an RSS feed for (or following) Tosback [5], a project of the Electronic Frontier Foundation [6], to track changes in website policies (which covers some, but not all social networks).
- Use caution when using third-party applications. For the highest level of safety and privacy, avoid them completely. If you consider using one, review the privacy policy and terms of service for the application.
- If you receive a connection request from a stranger, the safest thing to do is to reject the request. If you decide to accept the request, use privacy settings to limit what information is viewable to the stranger and be cautious of posting personal information to your account, such as your current location as well as personally identifiable information.
- Take additional precautions if you are the victim of stalking, harassment or domestic violence.
- Consider pruning your “friends” list on a regular basis. It’s easy to forget who you’ve connected to over time, and therefore who you are sharing information with.
- Log off from social networking sites when you no longer need to be connected.


Links