BRITISH COLUMBIA

Office of the Chief Information Officer

Top 8 Things You Shouldn’t Give Social Networking Sites

.....when signing up for an account, posting content or interacting with your contacts.....

Computer hackers, scam artists, identity thieves, debt collectors, stalkers, hiring managers and marketing companies are turning to social networking sites to gather valuable information. Take care that you aren’t risking your identity, security or reputation, and remember - the strongest tools users have to defend their personal privacy on social networking sites are common sense, caution and skepticism.

1	**Access to your email account** – During registration, social networks often ask a new user to provide an email address and account password so they can access the user’s email address book. To be safe, do not provide this information. Some social network companies will capture a user’s email contacts and then solicit them to join, which is unsolicited marketing. If you want to provide an email address and password to a social network, read all agreements, including the privacy policy, very carefully before proceeding.
2	**An email address associated with your professional life**. Never provide a work-associated email address to a social network, especially when signing up. Consider creating a new email address strictly to connect with your social networking profile(s). Jobseekers should take special care to keep professional and personal lives separate.
3	**Your exact date of birth, especially in combination with your place of birth.** Identity thieves know how to use this information to obtain identification in your name and even open bank accounts. A 2009 study at Carnegie Mellon showed that a date and place of birth could be used to predict most, and sometimes all, of the nine digits on one’s U.S. Social Security Number. If you do decide to post your birthday, don’t provide the year (it identifies your age) and use privacy settings to restrict the visibility of this information.
4	**Your browsing history.** Delete cookies, including flash cookies, every time you leave a social network site. Hackers can use them to learn the sites you have visited and the account names and passwords you have asked to “remember me” (which you should never do).
5	**Vacation Plans.** Do not publicize vacation plans, especially the dates you will be away. Remember, no matter how carefully you construct your privacy settings, this information can be used to invade your computer, or your home, in your absence.
6	**Public posts with your address, phone number or email address.** Don’t post these on a social network profile or status update. Scam artists and marketing companies are looking for this kind of information. If you do choose to post any of these, use privacy settings to restrict it to approved contacts. Be very wary of providing a GPS location of your home. If you use a “location aware” social network, use extra caution because people will know when you are absent.
7	**Compromising, sensitive, embarrassing or inflammatory pictures or posts.** Remember that whatever goes on a network might eventually be seen by people not in the intended audience. Think about whether you would want a stranger, an insurance company, the government, your mother or a potential boss to see certain information or pictures. Once it is on the Internet, you have lost control – it cannot be totally deleted
8	**Money.** Be wary of requests for money, even if they are from your contacts. If a contact’s account is compromised, a scam artist may use his or her name and account to attempt to defraud others through bogus money requests.

Source: Privacy Rights Clearinghouse http://www.privacyrights.org/

Revised October 2014