Staying safe on social networks

For businesses and employees, social networks represent a reputational risk, as well as presenting safety and security concerns. Google+, YouTube, Pinterest, Instagram, Tinder, LinkedIn and other social networks have become an integral part of daily lives and many employees use company systems to access social pages, providing hackers with an access route to sensitive information.

© mikkolem- za.Fotolia.com

1st for Women Insurance's Executive Head, Robyn Farrell, says, "It's very important to be careful how much personal information one divulges on social media or it can make one bait for criminals or stalkers."

Damaging one's professional reputation is another danger. "According to recent research on Forbes.com, 62% of employers use the internet to discover additional information about a job candidate. With this in mind, always think before you tweet or post pictures and information."

Guidelines for safe social interaction:

- There is no such thing as private. Everything posted or shared endures in the online environment. Even if it is deleted immediately afterwards, it has the potential to be captured by someone without your knowledge. Anything you put up can potentially be copied - not to mention hacked by thieves.
- Learn about and use the privacy and security settings on social networks. They are there to help you control and limit who sees what you post and manages your online experience.
- Be cautious about geo-location services, apps, Foursquare or anything that shares where you are. You home address can also be tagged unknowingly so check all the settings.
- Consider different social networking accounts for professional and personal life.
- Never share the year in which you were born. It provides an opportunity for identity theft.
- Keep track of privacy settings and check them on a regular basis or at least monthly. Do not assume that default settings will keep you safe.
- Make sure the privacy settings enable you to review content in which you are tagged by friends before it appears publicly on your page.
- Do not allow online games and other entertainment apps unfettered access to information.
- Never accept a friend request from someone you do not know, even if he or she appears as a mutual friend of a friend or several friends.
- Use a secure password that is different from the one for your email when you opens a new account. Change it frequently and do not enable auto-log in.
- Never allow an app to access to email or phone contacts.

Farrell concludes, "Don't be lulled into a false sense of security when it comes to protecting one's personal information. The goal of social networking sites is to generate revenue. Though the service may be free, there is the hidden cost of privacy. One must limit one's exposure and protect oneself. Social networking is meant to be fun, keep it that way by staying safe online."