Seven Security Tips for Social Networking

Social networking is popular, but due to the nature of social networking sites, there are potential security risks to you and the Department. Read these security tips to ensure that you don't subject yourself, your connections, or the Department to any risk.

What is social networking?

Online social networking is an extension of traditional social networking but is conducted over the Internet. Through purely social sites, you establish friendships or romantic relationships. Through business and special interest sites, you establish business connections and obtain information. Through your own blog or web site, you can keep others up-to-date on your work and personal endeavours. Social networking sites encourage you to provide a lot of information about yourself and they offer some type of communication mechanism (for example, chat rooms or instant messaging) that enables you to connect with others. On some sites, you can browse for people. On other sites, you must be "introduced" to new people through a shared acquaintance.

Why do we divulge so much?

When you reveal information online, about such things as a promotion or business travel schedules, you might provide more detail than if you were speaking to someone in person. In addition, you might not consider the probability of that information being misused or the impact of any misuse to yourself, other people, or the Department. Here are other reasons we tend to divulge a great amount of information online:

- The internet provides a sense of anonymity.
- The lack of physical interaction with others provides a false sense of security.
- We post information for friends or family, forgetting that anyone might see it–even cyber criminals and potential employers.
- We want to impress potential friends or associates by providing insight to ourselves and by mentioning the names of people we know, forgetting that we might be divulging too much information that others could misuse.
- We might not consider the legal or security implications of posting information about ourselves, other people, or the Department (now or in the future).
- We forget that the information is permanent and can never be completely removed from the public domain.

What are the security implications?

Most people using these sites don't pose a threat. However, malicious people are drawn to social networking sites because a large amount of personal, sensitive, and proprietary information is easily accessible.

People could collect information, bit-by-bit, and conduct a social engineering attack. In other words, they could impersonate you or cause harm to someone in the Department or to the Department itself. It's true that nothing malicious can usually be done, for example, with someone's name alone.

However, if someone knows your name, your address, a cell phone number, and birth date, then they might be able to convince someone that they have authority to access other personal or financial data. If you add a Social Insurance Number (SIN), then someone could open a bank account or secure a credit card in your name.

If you take a picture of someone at work, perhaps in a sensitive or restricted area and you post that picture to the Internet, you could be exposing information about that person or the location that shouldn't be considered "public knowledge". Remember, the more information malicious people have about you, your work, your connections, or the Department, the easier it is for them to take advantage of you, something you have, or something or someone you know. There are publicized accounts of operatives monitoring social networking sites to gather information for alleged terror attacks. The sites monitored contained pictures of people, places, and weapons. Many Foreign Service workers and militia have subsequently been ordered to remove information.

Seven Security Tips

1. **Limit personal information you post** - Do not post information such as your place of work or your schedule. Encourage your friends and colleagues not to post information about you. Don't take pictures or videos of your place of work.
2. **Remember that the internet is a public resource** - Post only the information you are comfortable with anyone seeing or which is allowed by your clearance. Remember this when you create your profile in blogs and forums. People you have never met can find your page. When you are keeping an online journal or blog, don't write it as though it were a personal diary; write it with the expectation that it is available for anyone.
3. **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with strangers, be cautious about the information you reveal.
4. **Be sceptical** - Don't believe everything you read online. People can post false or misleading information about various topics, including their own identities. Also, be sceptical about the security features of social networking sites. Security breaches are seldom publicized and no matter how secure sites seem, they could be exploited.
5. **Check privacy policies** - Some sites share information such as email addresses with other companies, which can lead to an increase in spam. Locate a site's policy for handling referrals to prevent unintentionally signing your friends or colleagues up for spam.
6. **Be careful what you advertise** - An increasing amount of personal information is available online. Whatever you decide to reveal, realize that you are broadcasting it to the world. When you provide details about yourself or others or post pictures or videos, you might be giving attackers enough information to perform a successful social engineering attack.
7. **Realize that you can't take it back** - Remember, after you post information online, you can't retract it. Even if you remove it, that information might be saved or cached on someone else's machine. **THINK** before you publish something on the Internet! Ask yourself what value it provides today and consider the implications of that information being publicly available now, and forever!