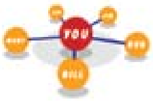
Social Networking Sites

1 *What are social networking sites?*



Social networking sites, sometimes referredto as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

Although the features of social networking sites differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, or email) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Some examples of social networking sites are Facebook, MySpace, Twitter and LinkedIn.

2 *What security implications do social networking sites present?*

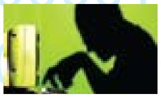
Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of personal information. When deciding how much information to reveal, children may not exercise the same amount of caution as they would when meeting someone in person because:

- The Internet provides a sense of anonymity.
- The lack of physical interaction provides a false sense of security.
- They tailor the information for their friends to read, forgetting that others may see it.
- They want to offer insights to impress potential friends.

While the majority of people using these sites do not pose a threat, predators are drawn to them because of the accessibility and amount of personal information available to them. Online predators may form relationships online and then convince young persons to meet them. The personal information can also be used to conduct cyberbullying.

3 *How can parents protect their children when using social networking sites?*

Although many of these sites have age restrictions, children may misrepresent their ages so that they can join. By teaching children about Internet safety, being aware of their online habits and by guiding them to appropriate sites, parents can make sure that the children become safe and responsible users.



Limit the amount of personal information posted - Educate your children to limit the amount of information they post that could make them vulnerable (e.g., full name, address, information about routines). If their friends or connections post information about them, make sure the combined information is not more than they would be comfortable with strangers knowing.

- **Remember that the Internet is a public resource** - Educate your children to only post information they are comfortable with anyone seeing. This includes information in their profile and in blogs and other forums.
- **Be wary of strangers and predators** - The Internet makes it easy for people to misrepresent their identities and motives. Educate your children to consider limiting the people who are allowed to contact them on these sites. Educate your children to be aware of potential online predators .
- **Check privacy policies** - As a parent, or teacher be aware that some sites may share information such as email addresses or user preferences with other companies and therefore children should be alerted to this potential hazard. Try to locate the policy for handling referrals to make sure that your children do not unintentionally sign up their friends for spam emails.

4 *Tips for children to socialise safely online*

Here are some things you can do to socialise safely online:

a. Think about how different sites work before deciding to join a site. Some sites allow only a defined community of users to access posted content; whilst others allow anyone and everyone to view postings.

b. Keep some control over the information you post by restricting access to your page.

c. Keep personal information private, or to a minimum. Keep your full name, social security number, address, phone number, and bank or credit card account numbers to yourself.

d. Make sure you keep not only your own information but other people's personal information private.

e. Make sure your screen name doesn't say too much about you. Even if you think it makes you anonymous, it doesn't take a genius to combine clues to figure out who you are and where you can be found.

f. Post only information that you are comfortable with others seeing and knowing.

g. Content posted to the Web can be copied, altered and reposted by anyone. Consider not posting your photo. It can be altered or broadcasted in ways you may not be happy about.

h. Flirting with strangers online could have serious consequences. Some people lie about who they really are.

i. Be wary if a new friend wants to meet you in person. If you decide to meet him, meet in a public place, during the day, with friends you trust. And tell a responsible adult where you're going.

j. If you feel threatened by someone or uncomfortable because of something online, tell an adult you trust, and then report it to the police.

NCB

CERT–MU

www.ncb.mu/sid