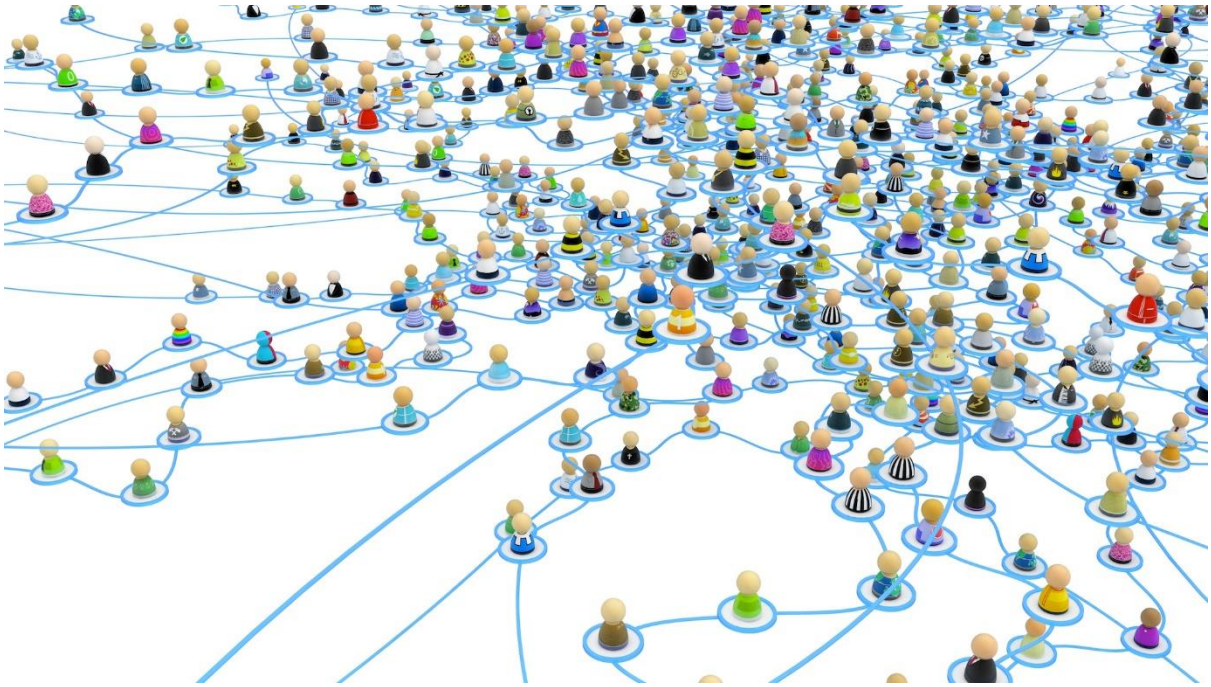
Cyber Smarts – Using Social Media Wisely

By Andrew Fuller



You have access to the world's largest museum, art gallery, library and social group ever created. You also have access to ways to expand your intelligence and your influence that your past generations could have never imagined.

To gain these massive benefits you need to have your wits about you and know how to use technology and social media wisely.

Accountability

Being completely anonymous online is a thing of the past. Anything that you share on social media, publicly or privately, can be tracked back to you and you may be held accountable for sharing it.

Always use the "Nana" rule

If you wouldn't want your nana, parents, teachers, or future employer to see something, don't share it on social media.

Illegal Content

There are some things that are entirely illegal to share on social media. Threatening posts and messages or "sexting" a nude photo of an underage person– even if that person is you– can lead to legal action and police involvement.

Privacy Settings

Know Your Audience

Know exactly who can see a post, picture or tweet before you share it. If total strangers can see all of your information, pictures, and everything you post, they can use this information to track you or to hack your profile.

Public versus Private

Privacy settings allow you to share appropriate content with friends and family while making sure that strangers can't access your information. Carefully choose what information you want people that you don't know to see when they view your social media profiles.

Private Isn't "Secret"

Just because you have a piece of information, a photo, or a post set to "private" doesn't mean that it can't be shared with others. While privacy settings make it more difficult for others to see things you don't want them to see, people inside your private network can still share photos and screenshots outside of the network.

Strangers & Online Friends

Know the Site

Some sites, like Twitter and Tumblr, are known for allowing people to connect and discuss art, music, politics and ideas with people from all over the world. Other social media applications, like Facebook and Snapchat, are almost always used exclusively for friends and family. Understand the culture of the social network before you join– it will help you make smart decisions about who to connect with.

Who to Friend

Strangers will occasionally send you friend requests on Facebook. Sometimes, they might even be from halfway around the world! No matter who they are or what they say, don't accept friend requests on Facebook from individuals that you don't know. Most people have a lot of personal information available on Facebook, and these strangers are looking for that information– not a new friend.

Don't trust everyone

Online friends can be valuable members of your social network– if they really are who they say they are. The Internet can be a great place to make friends with similar interests and from all over the world, but it is also full of people who are looking to take advantage of you.

Verify identity

Take action to make sure that anyone you interact with online is really who they say they are. Google's "reverse image search" can be used to check if a photo is really of that person, or if they stole it from an online source. Real people usually have fleshed-out profiles, visible interactions with friends and family members and lots of available photos.

Security

Secure passwords

Create a secure password keeps your identity secure, your personal information safe, and your accounts from being hacked. Choose a password that only you could think of, using information that

isn’t readily available on your online profiles. Every password should include both uppercase and lowercase letters, numbers and special symbols (!@#$%^*).

Choose your security questions wisely Sites often use security questions to help you reset a forgotten password. Hackers can use information on your social media profiles to easily answer these questions and gain access to your accounts. Choose security questions with answers that cannot be discovered by a quick scroll through your Facebook profile.

Location Tracking:

Any time you upload a photo online, there’s a chance that your location can be tracked through it. Most phones and cameras have GPS installed, and the information of your location can be found in the data of pictures taken on these devices. Websites can also track your location via your IP address.

Hackers

Most hackers use clues on your social media to discover your passwords and account details– or they may pretend to be someone that they’re not to convince you to tell them your information directly.

If You Think You’ve Been Hacked Change your passwords immediately; delete any posts that anyone else may have published on your account, and let your social network friends know not to open any suspicious messages from you.

Feeling Safe

Cyber bullying

Harassing threatening or intimidating someone else online is cyber bullying and it’s illegal.

If You’re Being Cyber bullied Don’t respond to any messages or posts that make you feel unsafe– use your computer’s screenshot function to take a picture of the message and show it to an adult that you trust.

Blocking Features

Most social networking sites have a block feature that can prevent another user from contacting you any further. Learn to use the block feature to stop a cyber bully in their tracks.

Reporting Harassment

Many websites allow their users to report other users who are sending harassing messages. Doing so may lead to the cyber bully’s account being disabled.

When to talk to an adult

Any time someone has made you feel unsafe online, it’s a good idea to talk to an adult about how to handle it.

Source; http://www.generationnext.com.au/2016/03/cyber-smarts-using-social-media-wisely/