



- Delete any messages of those who leave inappropriate comments.
- Use the privacy settings feature of the social networking site. It can help to protect your information and your friend's information. Set the "privacy" function so that people can only be added as your friend and view your profile if you approve it.
- Do not post information about your friends as you could put them at risk.
- Do remember what you post online is not private. Parents, teachers, and employers, may go online and find out about you.

As for parents to help their kids to use social networking sites safely

Kids and teenagers are seen to be more tech-savvy than their parents today. They are exposed to computers and internet in school but may not know the safety tips on various web applications they use that range from, email, chat rooms, online gaming and more. Parents cannot neglect their children while they are online and need to advise their children just like in real life, especially when dealing with strangers and giving information to others. Stalkers and other criminal are using website containing personal information to lure their victims, which kids are ever willing to post their information online without realizing the dangers. Kids find that social networking site as a platform to increase their circle of friends, apart from friends at school or their neighborhood.

The following are some tips for educating your children on making friends online safely:

- Monitor their activities on the Internet. You can monitor by installing some monitoring software to watch their online activities, e.g website they visit.
- They need to know what information should be kept private and not shared. Educate them on why such information should not be revealed. Citing real case scenarios or giving examples on what might happen can make kids look at it seriously.

- Tell them to inform you if someone asks or talks about sensitive issues or something that makes them feel uncomfortable.
- They should only post information that they or you feel comfortable with. Make sure that they understand the risks of posting personal information on these sites.
- Tell them the information they post online cannot be taken back.
- Enable privacy settings on the website to restrict who can post and access information on your child's site.
- Report to the site if you reasonably believe that someone is a scam artist or sexual predator on your children's profile site or on the social networking site in general.

INCIDENT REPORTING CHANNELS

Online Reporting

http://www.mycert.org.my/report_incidents/online_form.html

Telephone

Call Cyber999 Hotline number at 1-300-88-2999 or +603-8992 6969. Office Hours only. Monday – Friday, 8:30am - 5:30pm, GMT+0800

Mobile Phone

Call +6019-266 5850 (24 x 7)

SMS

Send SMS to +6019-281 3801

Email

Send email to mycert@mycert.org.my

Fax

Download form at:

http://www.mycert.org.my/en/services/report_incidents/fax_details/main/detail/157/index.html and fax to +603-8945 3442

CyberSecurity Malaysia

Level 7, Sapura @ Mines, 7, Jalan Tasik
The Mines Resort City, 43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.
Tel : +603 - 8992 6888 Fax : +603 - 8945 3205
E-mail : info@cybersecurity.my
www.cybersecurity.my



INFORMATION SECURITY BEST PRACTICE SERIES:

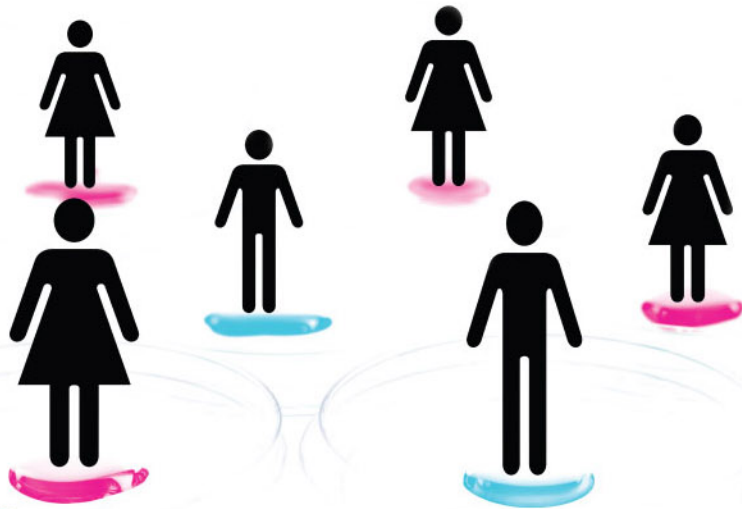
SOCIAL NETWORKING

CyberSecurity
MALAYSIA

An agency under MOSTI

Social networking has revolutionized the way people communicate, exchange information and participate in activities that explores interest of others.

Social networking has revolutionized the way people communicate, exchange information and participate in activities that explores interest of others. People with shared thoughts and interest come together in this ever growing medium. Social networking websites also employ the use of email and instant messaging services.



This platform enables people from near and far to communicate with their families, colleagues and friends. This platform has also opened up opportunities for businesses and entrepreneurs to build their contact database and use it as means to serve their customers. They can also promote their products and services using banner and text ads. Social networking websites are also widely used to network professionals together for meetings and information sharing.

Since social networking websites are laden with personal information and there have been growing concerns with people giving out too much of their personal information that gives cyber criminals opportunity to lure victims. Who needs to hack or dumpster dive when all they need to do is turn on the PC and log on to a social networking site. Social networking sites such as MySpace and Facebook have become an attractive target for cybercriminals looking to mine personal information, to trick users with phishing scams and spreading malware on exploited profile sites.

Yes, these sites are taking necessary steps by implementing security measures to minimize this problem, but users must still be cautious and aware. Necessary steps have to be taken by every user to protect themselves and their computer from threats as this involves their personal information and also information of their associates. They cannot just depend on the social networking sites to be responsible and do the job for them.

If that were not enough, time wasting and internet addiction can be another major setback resulting from these social networking sites. Children and teenagers, and even working adults may spend hours online modifying their profiles and communicating with others. Tasks and productivity may suffer as a result. Not to forget cyber bullying in which many websites let you rate another member's profile. This opens the opportunity for cyber bullying and allows nasty comments to be made. Negative comments can also appear in discussion groups and blogs.

The objective of this best practice is to provide useful safety tips to end users on the common threats and precautionary measures of social networking sites. On these sites, people usually share and exchange information, photos, videos, personal information, play online games, participate in interest groups, share thoughts, organize events, etc. It is one of the most engaging web applications of today as it is people-centric.

Tips to be safe when making friends online

- Beware of pretender and be vigilant. Potential exploiters can pretend to be someone else with a different age and background and convince you to add them as your "friend".
- Never share or post your personal information such as hand phone number, home/ work address in your profile. Potential exploiters use these profiles to search for victims.
- Be careful when posting text and image as it can be copied out by potential exploiter and in some cases, it cannot be taken back. Think before posting your photos as exploiter can use it to blackmail or threaten you. Personal photos should not have revealing information, e.g. your location.
- Never share your password with anyone.
- Add people as friends to your site only if you know them in person. Do not meet someone whom you have first "met" on a social networking site. People may not be who they say they are and this could put you in potential danger.
- Do not respond to harassing or threatening comments posted on your profile.