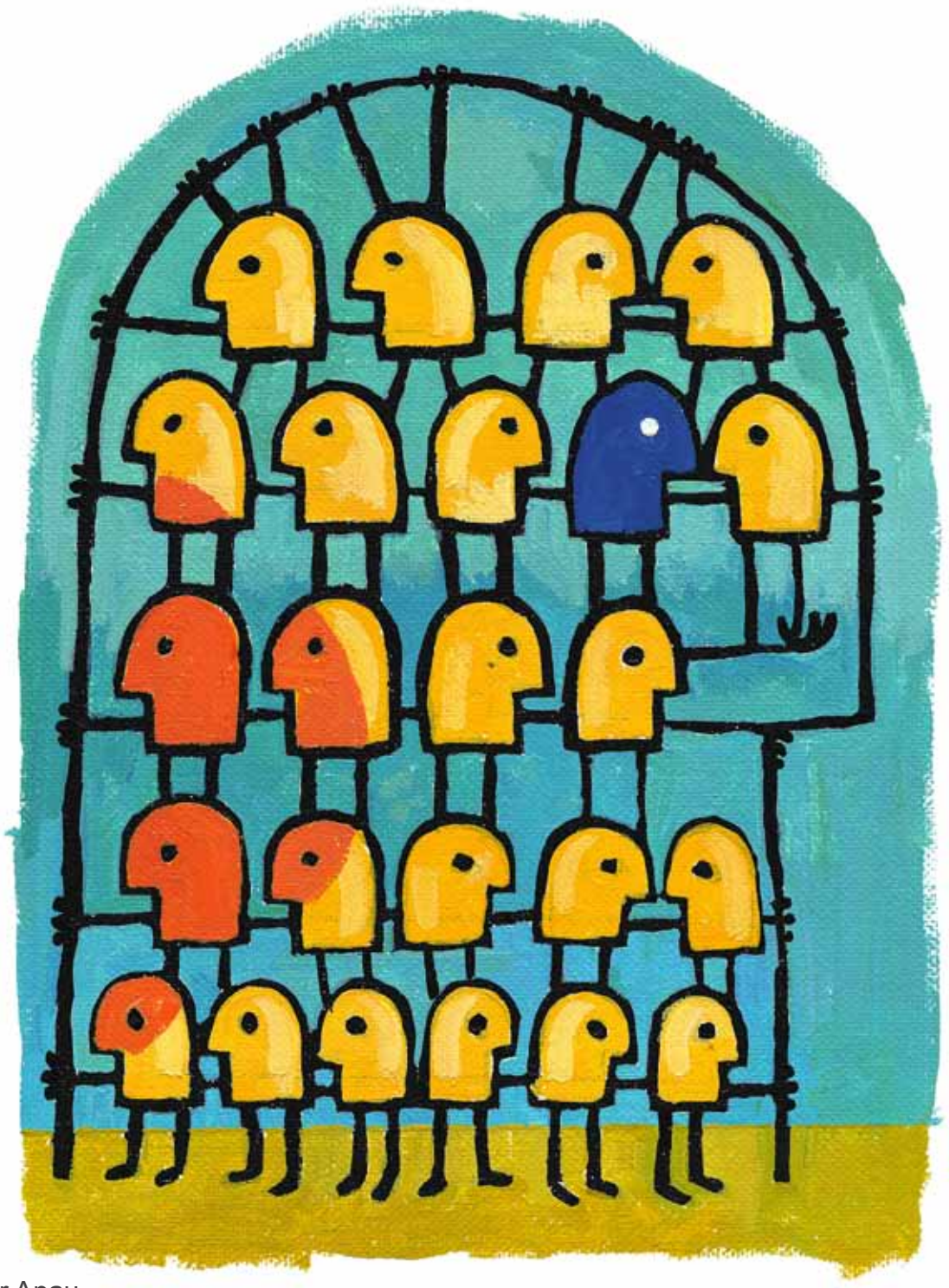
CyberSecurity MALAYSIA

AN agency under MOSTI

BEST PRACTICES ON

SOCIAL NETWORKING SITES (SNS)



Mohd Nazer Apau

COPYRIGHT

NO ENDORSEMENT

Products and manufacturers discussed or referred to in this document, if any, are presented for informational purposes only and do not in any way constitute product approval or endorsement by CyberSecurity Malaysia.

Registered office:
CyberSecurity Malaysia,
Level 7, Block A, Mines Waterfront Business Park,
No 3, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor, Malaysia
Phone: +603 - 8992 6888
Fax: +603 - 8945 3205
Web: http://www.cybersecurity.my

TRADEMARKS

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

WARNING AND DISCLAIMER

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on “as is” basis. The authors and CyberSecurity Malaysia shall have neither liability nor responsibility to any person or entity with respect to any losses or damages arising from the reliance to the information contained in this document.

ACKNOWLEDGEMENT

CyberSecurity Malaysia wishes to express gratitude to the contributors who may directly or indirectly contribute to the completion of this guideline. In addition, we wish to thank the panel of reviewers (Internal & External) who reviewed the drafts of this guideline.

Internal Reviewers

1. Adli Abd Wahid
2. Mohamad Nizam Kassim
3. Sabariah Ahmad
4. Sharifah Roziah Mohd Kassim
5. Sharifah Sajidah Syed Noor Mohammad
6. Security Management and Best Practices Department

External Reviewers

1.	Dr. Aida Mustapha	Universiti Putra Malaysia
2.	Jasmine Goh	Malayan Banking Berhad
3.	Khairul Shafee Khalid	Universiti Teknologi PETRONAS
4.	Ruhelmi Tasmir	Malayan Banking Berhad
5.	Suhanawati Salam	IKIP International College, Kuantan

Table of Contents

ABSTRACT

The Internet is a treasure trove. It provides an excellent communication platform through countless applications such as online forums, online chatting channels, video streaming, blogs and many more. All these are termed as Social Networking Sites[1] (SNS) or Social Media[2]. Considered to be the greatest technological innovation ever discovered, Social Media is fast gaining popularity globally among Internet users. U.S. President Barack Obama went as far as to compare social networking to universal liberties such as freedom of speech.

With the current Web 2.0 technologies and the evolution of Web 3.0, SNS are going beyond the horizon of recognition and reception for humankind. Popular SNS like Facebook, Twitter, MySpace, LinkedIn and YouTube are providing improved mediums for interaction as compared to traditional methods (e.g. face-to-face). Without boundaries, humans can share and exchange ideas, disseminate information, express emotions, inspire others, transpire ideologies and the list continues. On top of that, most corporate and enterprise companies feel that the emergence of SNS should be treated as opportunities in capturing and sustaining customers through cost saving marketing tools and getting direct feedbacks. Even politicians are seriously considering SNS as effective campaigning tools and provide them with a platform to appear closer to their supporters.

Unfortunately, SNS does not always provide a positive outcome and the desired benefits. This best practices document is going to draw your attention on the possible impacts of using SNS and eventually suggest relevant guidance. At all times, this document should be treated as best practices and as a supporting guide for your current organisation's internal policies and procedures.

[1] A social networking service is an online service, platform, or site that focuses on building and reflecting of social networks or social relations among people, who, for example, share interests and/or activities. A social network service essentially consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web based and provide means for users to interact over the Internet, such as e-mail and instant messaging. (http://en.wikipedia.org/wiki/Social_networking_sites)

[2] The term social media refers to the use of web-based and mobile technologies to turn communication into interactive dialogue. Social media are media for social interaction, as a superset beyond social communication, but mainly still communicating just interactively using ubiquitously accessible and scalable communication techniques. (http://en.wikipedia.org/wiki/Social_media)

INTRODUCTION

This document will be referring mostly to Facebook and Twitter as the point of reference for Social Networking Sites (SNS) and Social Media due to their popularity and being the most popular medium used by many Internet users nowadays. Nevertheless, the potential impacts, risks and guidance that are going to be discussed in this best practices document are basically applicable to all type of SNS and Social Media applications and are not limited to Facebook and Twitter alone. It is our hope that by producing this (best practices) document, it will provide the necessary awareness and mitigation towards the potential risks and impacts that a user might experience.

Astonishingly, Facebook accumulated almost 700 Million users worldwide as of June 2011. If we were to consider Facebook as a country, it would be the 3rd most populated nation after China and India. Last year (2010) alone, Facebook recorded 7.9 users registering every second. In terms of user growth on Facebook, Malaysia is ranked at the 11th spot while Brazil is ranked 1st and Japan is ranked 20th respectively[3].

#	Country	Facebook users	Growth [abs]	Growth [%]
1.	Brazil	19 091 140	1 949 700	11,37
2.	Indonesia	37 867 700	1 509 600	4,15
3.	Philippines	24 501 880	1 332 580	5,75
4.	Mexico	24 770 160	1 119 520	4,73
5.	Argentina	15 111 480	1 067 960	7,60
6.	India	25 771 360	918 140	3,69
7.	Colombia	14 262 440	909 940	6,81
8.	Egypt	7 934 080	795 280	11,14
9.	Turkey	28 937 140	727 220	2,58
10.	United Kingdom	30 556 020	661 200	2,21
11.	Malaysia	10 884 680	576 660	5,59
12.	Germany	18 686 280	487 560	2,68
13.	Italy	19 631 700	460 520	2,40
14.	Venezuela	8 913 120	455 500	5,39
15.	Peru	5 912 200	438 320	8,01
16.	Belgium	4 509 040	402 140	9,79
17.	Chile	8 400 060	397 260	4,96
18.	Thailand	9 516 120	389 180	4,26
19.	Spain	14 140 240	339 840	2,46
20.	Japan	3 397 240	283 660	9,11

Table-1: Top Growing Countries in May 2011 on Facebook
source: Data manually collected on Socialbakers.com

In Table-1, it reflects that all countries are clearly contributing a positive growth. With that information, SNS (particularly Facebook) are creating huge opportunities for the good and the bad guys to have leverage on them. On the negative side, MYCERT[4] of CyberSecurity Malaysia recorded about 324 cyber incidents related to Social Networking Sites. In Q1 2011 alone, there were about 177 related incidents (cases) reported to MyCERT. The rise in the number of reported cases are in tandem with the increase of SNS users (usage).

We can consider SNS as a double edged sword. If we use it wrongly, it can harm us (and others too) and if we use it wisely, it can be of immense value to us (Marketing Strategy, Branding, Mass Media, Information Sharing, Humanitarian Causes, etc). In this best practice document, we invest our expertise to ensure Internet users understand the adverse effects of using SNS. By knowing and understanding the undesirable effects of SNS, it could assist us and the people that we care to avoid becoming victims of digital perpetrators.

[3] http://www.socialbakers.com
[4] http://www.mycert.org.my/en/

POSSIBLE IMPACTS OF SOCIAL NETWORKING SITES

The possible impacts outlined below are not the only negative effects that could strike us as SNS users. However, these impacts could lead to multiple consequences which may not be discussed in this document. The existence of further potential exploitation and manipulation by perpetrators are always against you, along with the people that you care. For that matter, understanding the potential impacts (negative effects) and risks would enlighten us to be more prudent and restrict ourselves when putting our information online. It could also lead us to improve the current state of our actions in overcoming SNS threats. Parents and adults are expected to share the understanding from this document with their family members and particularly with children. Furthermore, both parents and adults play an important role to inculcate the message conveyed by this document to others who do not have the opportunity to read it.

1. Cyber Bullying & Stalking

Harassment perpetrated via the Internet, cell phones or other devices can be considered as cyber bullying[5]. SNS can be used as tools (technology) to intentionally harm others through hostile behaviour such as posting nasty comments and unruly pictures on SNS individual's page. In addition to that, these channels can be used to stalk people. Cyber stalking is a crime in which an attacker harasses a victim using electronic communication (in this case a SNS channel). A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victims without being detected[6].

Nonetheless, children are not the only possible victims of Cyber Bullying and Cyber Stalking. The same risks could apply to adults as well. Victims may be intimidated and potentially lose their privacy and can suffer from physiological trauma. It could possibly cause physical harm or injury to the victim as well. Some users may unwarily (or choose to be ignorant) use part of SNS application that directly notify the public of his or her whereabouts. This could definitely present tremendous advantage to the stalkers and criminals.

[5] http://definitions.uslegal.com/c/cyber-bullying/
[6] http://searchsecurity.techtarget.com/definition/cyberstalking

2. "Phising[7] Ponds"

The increase of SNS and users provide more avenues in supplying abundance of information to your "trusted friends". In this context, "trusted friends" mean your friends in the list that you never verify or knowing them personally. Subsequently, it can be the opportunity for perpetrators to "phish". The chances of people putting their information (credentials) and being unaware of the dreadful consequences are very high. This is where the bad guys may use social engineering[8] techniques to lure their victims into putting more and more valuable information online. Victims are normally tricked to put their data that may be valuable information for the perpetrators. These perpetrators also prey on a victim's account or compromise systems for other purposes like identity theft and persistently looking for users who inadvertently (unaware) reveal their Internet banking details and other useful particulars.

3. Subject to Manipulation and Exploitation

With the abundance of information from the available "ponds", perpetrators look for chances to manipulate and exploit it. The information can be downloaded and stored remotely where formation of database can be done and properly structured. Images, videos, links and other useful information are difficult to completely delete since people could always tag and comment on it. You may think that you have securely erased the information but somehow it may already be downloaded and saved by others. You do not want your pictures and any of your family members to fall into the wrong hands and later be shared amongst them.

To make it worse, with current and future technology, images can be linked to form useful information for these attackers. The face and object can be recognised through a high-end application and lead to your whereabouts and form more useful information for the bad guys. In addition, tagging the image with metadata can reveal constructive information like timestamp as well as email address.

4. Privacy Violation

The fact that you are interested in reading this document signifies your recognition towards SNS. The media is considered as an excellent communication channel. However, not many of us are aware that in general SNS are not always protecting our security and privacy as many people expect it to. Humans (SNS users) tend to share many things with others whom they trust. Without carefully configuring an appropriate "privacy" setting, postings on your wall, pictures or profile may be exposed to a person that is unknown to you.

Furthermore, mobile phones are now mostly equipped with a camera. It is common that with the same hardware, the owner usually installs SNS applications on it. Due to the handiness of using SNS, a friend might spontaneously take your pictures and relentlessly post it on the web without you noticing it. What happens if the picture that was taken was not actually appropriate for public viewing? We know that pictures can describe many words. Hence, it is very likely that your pictures could end up in cyberspace without you knowing it and potentially damage your reputation.

---

[7] Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is similar to Fishing, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. But the hook inside it takes the complete fish out of the lake (http://en.wikipedia.org/wiki/Phishing).

[8] Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim (http://en.wikipedia.org/wiki/Social_engineering_(security)

5. Corporate Espionage

The risks of information leakage and exposing trade secrets to competitors are always possible from the SNS perspective. Attackers may come from your "trusted" friends and take advantage by conducting Corporate Espionage. They are normally capable of gaining inside information through social engineering techniques from those SNS channel. Corporate Intellectual Property and information could unwillingly surrender to other parties and competitors through SNS channel. Unknowingly, certain information posted through SNS could also lead to further damage like physical intruder access, corporate networks being hacked, ransom demands as well as extortion.

6. Risk of Losing the Legal Battle

Organisations that realise the risks of corporate espionage will agree that the best countermeasure is probably policy and awareness. Unfortunately, not many companies are looking at current policies on whether or not it sufficiently exists to protect the organisation in cases of breach resulting from related SNS usage. Employees could always claim that they are not aware of such situations if awareness is not implemented. Furthermore, without proper policy and dissemination to the staff, it reflects on the lack of due diligence from the organisation.

7. Productivity Loss

SNS can create pleasure and therefore it engages users to waste their time and prevent them from doing other productive activities. Organisation that allows its staff to access too much of SNS like Facebook, Twitter, and Youtube in the office premises and during office hours could experience productivity losses. Furthermore, with SNS' streaming videos, online chatting, games and other unproductive applications, chances of having bandwidth issues in the organisation's network could definitely increase. It would disrupt the legitimate use of applications and transactions within the same network.

Adults and kids could face the same productivity loss as well. Adults may face the same productivity loss when they spend too much of their time on SNS. Supposedly, they can do other things like sports activity, family outing, chatting with offline friends, and other productive activities instead of surfing the Internet and SNS. Children's health-risk and psychological condition could also be significantly affected whenever they spend too much of their time on the Internet and SNS.

8. Viruses and Malware

SNS can turn into excellent avenues for viruses and malicious software (malware) to penetrate your application and network systems. Those are included but not limited to your mobile phones, notebooks, desktops and servers. Lack of awareness from the adults and a child's curiosity (Youth, Kids) is the main reason why malware remain strong and attack from this channel. The corporate networks are susceptible to this attack where it could lead to more harmful consequences like data losses, data theft, system unavailability and network as well as application hijack. In addition to that, unnecessary resources (staff) need to be allocated to clean up. It could definitely cost a huge financial implication if the outbreak contaminates most of the organisation's network segments.

GUIDANCE OF USING SOCIAL NETWORKING SITES

The possibilities of the impacts happening to you can be mitigated with the guiding principles below. In addition to that, avoiding yourself from becoming the victim can come from few perspectives, such as securing your devices (Computer, Laptop, Smartphone, Tablet PC, etc.), Internet connection, browsers, SNS account, application, and the human element itself. This document taps more on the human element perspective as we feel that it is important to tackle it promptly since it is perceived as the weakest link in any form of security issues. To err is human, but if you could apply these principles whenever you are dealing with the usage of SNS in your daily life, it could definitely put yourself in a safer situation. This section outlines 10 guiding principles that you can practice and extend to others. By doing so, it would reduce the risk of you and your loved ones becoming victims of perpetrators. All principles discussed in this document are related to COMMON SENSE, as we mention at the end of this section.

1. Be cautious about personal and business agenda

It is common for any organisation to have the employee handbook which explains the “dos” and “don’ts” for staff. Make sure you read and understand what is inside as it is important as a staff to be aware of the content of the handbook. Furthermore, staff should be familiar with the organisation’s policies, procedures, guidelines and code of conducts. By doing that, staff will certainly be conscious of what “can” and “cannot” be posted/twitted through SNS. If you are not sure about something, the safer route is to defer your thoughts and get the opinions of your superior or human resource personnel prior to posting/twitting on the subject.

Organisation may encourage the usage of SNS for brand recognition, brand awareness, interaction and communication facilities with customers, marketing, product promotion , organizing a contest, services, advertising and a lot more. While maintaining the organisation’s mission, organisation must make sure the SNS policy exist in the company. With the available policy, staff could adhere to it. However, organisation must not forget on having effective policy enforcement.

2. Be Objective

The first thing you should do is to ask yourself on the reason for having SNS account like Facebook, Twitter, MySpace, Linked-In and any other type of SNS. If you are using it so that you are informed and updated about your friends, then let’s be sure about it. Accept only “friends” that you know directly and not the one that says they “know” you. You have to firmly decide on how you are going to use SNS for your own sake and benefit. Otherwise you will be “drowning” with the hype and excitement of using SNS. If your children have it, do take notice and ask them about their friends and what they normally do when browsing SNS.

Users don’t have a good rationale for having thousands of “friends” in their list. Exception for those who are basically collecting “people” for product marketing purposes and/or if the person is considered a “celebrity”. They might have a good reason to have massive list of “friends”. Unlike the regular SNS users, you should probably revisit your friend’s list and review whether or not it needs to be profiled. Once you have done the profiling of your friends, it is a lot easier to enforce distinct rules on each group.

But, for those who maintain enormous list of "friends", you still have to be guided with the rest of the following principles. For professional references (Linked-in), be sure to accept someone that you have worked with directly. In the case of professional and non-professional bloggers, they need to be clear on his or her objective when having their blog/website. While maintaining the objective, bloggers should respect the local law and be responsible on what is posted on his or her blogs.

Another interesting area to consider is whether to use your actual name or pseudo name. Again, it goes back to your objective of having SNS accounts. It is a bad idea to remain anonymous. After all, it defeats the purpose of "connecting" with people. But, if you prefer to use pseudo name, it is very important to make sure that your "circle of friends" is aware that it is you. By doing so, your friends can positively react towards you. In other words, as long as you remain (behave) as who you are, and not pretending to be someone else, then it should be fine.

3. Think before you "post"

What you post as information, pictures, videos and other things (attachment) through Social Networking Sites, will be available to many viewers. Literally, the information that you post will forever exist in the cyber world since it can be shared, downloaded and uploaded again by another person. Perpetrators could manipulate the information you posted and harm you in certain ways. Remember, it can haunt you in the future if you do not "think" for a moment before posting it. Thus, do not post images, pictures and information that can humiliate you, family, friends, the customers and the organisation as well.

As an employee for an organisation or institution, you must be clear with your role and whether or not information that you post is confidential or may potentially breach the organisation policies and code of conducts. If you are not sure with item that you want to post, DON'T proceed for posting. In short, be clear on what you want to post and the possible consequences.

4. Think before you "Click"

You may have the tendency to click every link that seems to be genuine from a "friend" and you never thought that a "friend" would do something terrible to you. However, be wary of some links that may harm your computer and organisation's network, which are willingly or unwillingly shared from your friends. It is best if you could copy the link and paste it into the search engine (i.e. Google, Yahoo and Bing) and analyze the outcome. It may tell you that the links basically contain a harmful result. This two minutes job could save you from hours of clean up if an outbreak occurs.

5. Don't expect your privacy is protected.

It is important to understand that privacy is not the top priority when Social Networking Sites like Facebook, Twitter and MySpace were invented. After all, posted information is basically meant to be available for everyone who can access the Internet.

Hence, it is not the best practice to trust the "Privacy Default Settings" since SNS were made to cater to bigger crowd with different types of people and background. Do analyze the default setting and set it "right" for you. You must read the SNS' Terms and Condition (T&C) as well as Security and Privacy setting from the SNS provider. By doing so, you will at least be aware on the T&C and be able to make a smart decision about it.

6. Have a "strong" password

You must make sure to use a strong and hard-to-guess password for your SNS account. The best password is to use up to 14 characters with mix upper and lower case characters, numbers and symbols. The user id and password must not be shared with anyone, no matter how close the person is with you. This would reduce the risk of perpetrator hijacking your SNS's account. In addition to that, it is best to not have the same exact password from your online banking and any other online application. Don't forget to change the password periodically (recommended every 6 months) and keep it in a safe place. The best is to memorise the password so that you will not have to write it down and accidentally display it at a visible place.

Another important point to note is to never-ever reveal your password through email or anything else similar to it. It is very rare that you are needed to reveal your password to a support team, application or service provider. In case you are being requested to reveal it, it is very likely that you are being tricked by a perpetrator through a social engineering technique.

7. Anti Virus or Anti-Malware installed and updated

Ensure that Anti Virus or Anti-Malware (Internet Security) is installed and updated with the latest patch. It is very important to have it installed in your notebooks, desktop and servers in order to mitigate the risk of virus and malware spreading throughout your machine and organisation's network. In addition to that, all machines must also be equipped with updated application and Operating System patches.

8. Never ever reveal anything related to PII

PII stands for Personal Identifiable Information[9]. By any chance, DO NOT put anything that is related to you and your personal information in the Social Networking Sites or any public website (That is inclusive of other person's PII). Children need to be reminded of this as they may not understand about sensitive information and the consequences. Parents and adults must adequately monitor their children (the Youth and the Kids) whenever they are online. This is to ensure children are free from being the victim of Cyber Bullying and Cyber Stalking.

9. Have a tool to filter and scan the SNS

Organisations that allow the usage of SNS while at work, should invest some technology like filtering tools and malware scanner to ensure the contents, links and attachment files are free from viruses and malware. The contents allowed should be harmless to the users as well as to the corporate network. Nevertheless, be wary that it only works as well as intended if the person is well trained and skilful to man the technology. You cannot expect the technology to resolve the problem if it is not implemented correctly, maintained properly and updated frequently.

10. Try to limit your "time" with SNS

You have to be in control whenever you are using any part of the SNS or social media channel. You must allow yourself to limit certain maximum hours to spend on SNS. Otherwise you are at risk of becoming addicted and spending too much time on Facebook and any other SNS. It can contribute to a negative effect on you and the people close to you.

Get your friends, family members or the person whom you trust or probably yourself to assess whether you are addicted to SNS particularly Facebook. The person who is closest to you is the best option to give feedback about your behaviour towards SNS. They might feel neglected and ignored by you because of your time with Facebook or any other type of SNS. Furthermore, people who are addicted to SNS will have the tendency to ignore the rest of the following principles. So, it is important to make sure that you are not one of them. In other words, stay away from being addicted. As for the children who are not being monitored by parents and adults, they are in a dangerous situation to occupy most of their productive time with Internet and SNS. Therefore, parents must play a vital role in making sure the children are not having too much time "talking" to their on-line "friends" and excessively browsing the Internet and SNS.

[9] Personally Identifiable Information (PII), as used in information security, refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. The abbreviation PII is widely accepted, but the phrase it abbreviates has four common variants based on personal, personally, identifiable, and identifying. Not all are equivalent, and for legal purposes the effective definitions vary depending on the jurisdiction and the purposes for which the term is being used (http://en.wikipedia.org/wiki/Personally_identifiable_information

COMMON SENSES, PLEASE!

Apply a common sense to your desire. You may want to put every single detail of information for your “friends”; but do they really need to know all that information that you want to post? Never, ever put information related to your financial standing, specific home address, children’s detail and contacts, their pictures, health information, personal information and conversation, and other information that you do not want the public to know about.

For those who basically like to use applications that broadcast on “where you are”, probably you should reconsider whether it is necessary. By telling others “where you are”, it is giving privilege to strangers to stalk you or inviting the bad guy to rob you (whenever you are not at home). As highlighted earlier, some people like to use “not-the-real-name” for his/her profile. Whatever the reason is, be sure your “friends” that you invited or befriended know who you actually are. You and your friends should not accept friends that you do not recognize or know.

In this regards, adults as well as parents are responsible to make sure their children do not overly expose their information as well as their family information. Parents and adults must play their role in monitoring and giving appropriate advice to children. In addition to that, children need to be encouraged to seek assistance from parents whenever they are unsure about anything related to SNS usage. Please apply C.O.M.M.O.N. S.E.N.S.E. as below.

Cautious Engagement – careful with what you “post” and “click”
Objective Perceptions – know the “why” you engage with SNS
Match Intentions – stick to your objective
Mark Policies – read internal (organisation) policy and T&C of respective SNS
Organise comrades – profile your “friends”
Never Assume – do not expect your security and privacy is preserved

Strong Passwords – good combination of password’s characters
Extreme Fortification – equipped your notebook, desktop and servers with anti-malware
Nurture Secrecy – never ever reveal anything personal. i.e. PII, self and family particulars, address, private number, etc.
Secure the Password - keep password at “safe place” – memorize without writing it
Excellent Safeguards – equipped your organisation with relevant filtering tools / technology
Self-Restraint – stay away from being addicted

CONCLUSION

Social Networking Sites and Social Media are used interchangeably. The two can carry different meaning but in the context of this document, it both can carry negative consequences and the same precautions are needed to overcome that. What were discussed in this document are not exhaustive and should not be perceived as the only issues and challenges faced by humankind. This document should be able to open our mind and make us more cautious about the consequences discussed, and possibly think further about other consequences that were not discussed. There is no silver bullet to overcome the issues and challenges emerging from the SNS. Users must extend their knowledge and awareness on safe browsing principles and keep updated with the best practices on using SNS or social media. Perpetrators are always looking for the opportunity to manipulate and exploit information for their own benefits. That in return, will cause some unfortunate incident to anyone who allowed him/herself to become a victim. We must always keep ourselves updated with the latest threats, tools and technology relevant to the SNS in order to avoid the misery of becoming the victim. The Appendixes present some useful tools and links that can be used as stepping stones for you to learn more and be cautious about related SNS and social media issues and risks.

Also, there are many tips and advices to follow whenever you are online and surfing the Internet which can be found from the Malaysia CyberSecurity website through its CYBERSAFE[10] portal.

[10] http://www.cybersafe.my/2011/index.html

APPENDIX A: EXERCISING THE 5Ws and 1H

The 5Ws1H Questions can be used to gather basic factual information related to your “friends”. These questions are not meant to provoke the current “friendship”, but the main purpose is to make you aware on who are available in the list and reconsider whether or not to put them in your “trusted friends”. Facebook allows you to “profile” your “friends” so it would be easier to enforce distinct privacy to each profile (http://www.facebook.com/help/?page=768). What do you need to do now? You can start by going through your friend’s list (Facebook), and try to answer each of the questions below.

1. Who is he/she?
2. What is his/her real name?
3. Where do you know him/her?
4. When did you start to know him/her?
5. Why are you accepting him/her in your “friend” list?
6. How is he/she looks like?

Can you achieve to answer each question? Are you in doubt about your “friends” then? You may need to consider removing him/her from the list if you cannot answer any of the above questions. <The same methods could apply to any of your other SNS as well>.

APPENDIX B: USEFUL LINKS

Sample Social Media Policy, Procedure, Guideline, and good tips related to Social Networking Sites / Social Media **(Last accessed on June 16th, 2011)**	1. http://socialmediagovernance.com/policies.php 2. http://www.ibm.com/blogs/zz/en/guidelines.html 3. http://blogs.law.harvard.edu/terms-of-use/ 4. https://wiki.internet2.edu/confluence/display/itsg2/Social+Networking+Security 5. http://www.microsoft.com/security/online-privacy/social-networking.aspx 6. http://www.makeuseof.com/tag/10-twitter-safety-tips-to-protect-your-account-identity/ 7. http://support.twitter.com/groups/33-report-a-violation#topic_121 8. http://www.sophos.com/en-us/security-news-trends/best-practices/facebook.aspx 9. http://www.facebook.com/privacy/explanation.php
Profiling your "Friend" (Last accessed on June 16th, 2011)	10. http://www.allfacebook.com/facebook-privacy-2009-02 (10 Privacy Settings Every Facebook User Should Know)
Privacy Setting Tools (Last accessed on June 16th, 2011)	11. http://www.reclaimprivacy.org/
Password Generator & Password Checker (Last accessed on June 16th, 2011)	12. http://www.pctools.com/guides/password/ 13. http://strongpasswordgenerator.com/ 14. http://www.passwordmeter.com/ 15. https://www.microsoft.com/security/pc-security/password-checker.aspx

APPENDIX C: SOURCE OF REFERENCES

1. Social Media: Business Benefits and Security, Governance and Assurance Perspectives (An ISACA Emerging Technology Whitepaper)
2. Giles Hobgen et. all, Security Issues and Recommendations for Online Social Networks, ENISA, 2007
3. Social Media in the enterprise: Great Opportunities, great security risks – SOPHOS (June 2010)
4. Jarkko Rantamaki, Perceived user value of social networking, Helsinki U, 2008
5. Prof Steven Furnell, Social Networks – Access All Areas? , Computer, Fraud & Security, May 2011
6. Jim Mortleman, Social Media Strategies, Computer, Fraud & Security, May 2011
7. FactSheet – Secure on Social Networks Version 1.1, April 2011
8. The Social Media Taskforce, Reed Smith, Social Media Risks and Rewards, 2010
9. Catherine Everette, Social Media: Opportunity or Risk? Computer, Fraud & Security, June 2010
10. Price Waterhouse Coopers – Security for Social Networking, February 2010

BEST PRACTICES ON
SOCIAL NETWORKING SITES (SNS)

This best practice document is created for all Internet users who occupy themselves with Social Networking Sites or Social Media in their day to day usage. It suggests some best practices that can be applied by Social Networking Sites (SNS) and/or Social Media users to alleviate the risk of becoming the victim of perpetrators. The possible impacts (not exhausted) highlighted in this document can be mitigated with a simple practice of C.O.M.M.O.N S.E.N.S.E.S

CyberSecurity Malaysia,
Level 8, Block A, Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan,
Malaysia.

Tel: +603 - 8946 0999 Fax: +603 - 8946 0888
Email: info@cybersecurity.my
www.cybersecurity.my

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

ISMS SIRIM
CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

STANDARDS MALAYSIA
ACCREDITED LABORATORY
MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

MSC MALAYSIA
Status Company