



Social Media

Security – Best Practices for General User

China has become by far the world's most active social-media population, with 91% of respondents saying they visited a social-media site in the previous six months, compared with 30 percent in Japan, 67 percent in the United States, and 70 percent in South Korea (Mckinsey).¹

Being part of the social media community has its benefits. Social media allows users to remain in contact with loved ones and friends who live far away. It is also a great tool for getting informed fast. Meeting people from all over the world and sharing opinions has never been so easy. The distance between people seems to be closer. For example, you can have net-friends who are living in United Kingdom, France or Australia; you do not need to visit them by traveling but just one click of their online profile and take responds.

Social Impact and Privacy Concern

However, there is also a downside to social media. Many people have become addicted to their online lives. The lack of privacy that has evolved from this has also become a topic of concern.

Things posted on social media can intrude privacy which should be a topic of concern. For example, a simple birthday invitation becomes an online invitation where people can see how many friends are invited and who is going. The music a user listens to in Spotify is advertised by Spotify through social media to the user's friends using the user's name and profile picture. If a user "likes" a news article or a simple clothing offer, it can be potentially shown to the user's friends. This is how social media is kept free - through Nowadays, smartphone is the most popular channel for people connecting with social media. The statistics from U.S. in March 2012 shows that

advertisements. The more you share and "like", the better will be for business because the social media companies have the intelligence to analyse or sell to third-parties. It is important for users to understand their privacy rights when using social media so as to decide how to protect personal and private information, and even opt out of certain social media offerings.

Besides advertisement and privacy issues, there are reported incidents about kidnappings, robberies and identity theft cases which are made possible because of social media. The vulnerability and innocence of students have also been taken advantage such as students agreeing to meet with strangers over social media invitations. Cyberbullying using social media are also increasing - videos and obscene texts are posted online making fun of or insulting victimised teenagers by other students. Users are therefore reminded to be careful and cautious of what to post and share over social media.

It is also imperative to understand both the good guys and bad guys are using social media to browse people's information. Governments and law enforcement may gather such intelligence for legitimate reasons such as fighting terrorism. If a social media company receives a court order to release information about a specific user, the company will be obligated to release such information. Criminals may create spear phishing email attacks based on the target's profiles published on social media. Whether these social media browsing activities are for legitimate reasons or not, these could mean invasion of privacy.

The Whistle Blower

The leaked out documents Edward Snowden, U.S. National Security Agency contractor, reviewed that U.S. Government is using social network data stores to go through people's personal information. While this is used to gather intelligence about terrorists who pose threats to homeland security, it is also a huge violation of privacy.



Facebook was the most popular social media apps for people connecting with social media, with the average Facebook mobile user engaging for more than 7 hours via browser per month.

| Selected Social Networking Properties (Mobile Browser and App Audience Combined) March 2012 Total U.S. Smartphone Subscribers Age 18+ on iOS, Android and RIM Platforms Source: comScore Mobile Metrix 2.0 | | | |
|---|-----------------------------|---------|-----------------------------|
| | Total Unique Visitors (000) | % Reach | Average Minutes per Visitor |
| Facebook | 78,002 | 80.4% | 441.3 |
| Twitter | 25,593 | 26.4% | 114.4 |
| LinkedIn | 7,624 | 7.9% | 12.9 |
| Pinterest | 7,493 | 7.7% | 52.9 |
| Foursquare | 5,495 | 5.7% | 145.6 |
| Tumblr | 4,454 | 4.6% | 68.4 |

Social Media & Smartphone²

It could be a concern for students and teenagers when using smartphone to engage into such kind of prolonged social media activities. Criminal can plan some forms of scam via this channel to gain trust with their targets in order to carry out nefarious activities to make profits and commit crimes. Parents should pay attention and teach their children how to protect themselves out of any possibly scam activities and able to discern the kind of behaviour that may violate privacy and laws by using social media.

What Exactly are Social Media?

Social media can be defined as communication platforms with their own specific social practices and where content is generated by the public.

SOCIAL NETWORK

Social Network were originally envisaged to create circles of friends and search for business partners, jobs, etc. by means of tools that let people present themselves, communicate and interact. Examples: Facebook, Google+, LinkedIn, Twitter, Viadeo, etc.

FILE SHARING SITES

These platforms let people share media in the form of photos, videos, presentations, etc. Examples: Dailymotion, FlickrR, Picasa, SlideShare, YouTube, etc.

BLOGS

Blogs are a place for people to express themselves online. They are typically participative, allowing people to comment, react and engage in discussion. Articles are published and archived in reverse chronological order (the most recent post appears first) and allow all visitors to respond to the topic and the issues raised by posting comments, thereby creating a close relationship between author and readers.

There are also forums, virtual universes, MMOs (massively multiplayer online games), blogs, wikis, livecasts and much more.

The Most Popular Social Media

The following social media are now commonly used by people:



Twitter has huge power in controversial issues. People talk live about current events and thus, just as news and opinions travel fast, rumors can also spread.

Twitter has 500 million users. It lets you send brief messages called tweets, limited to 140 characters. Twitter is easy to use, which is partly why it's so popular.

It has its own language and practices, such as retweets (RTs), Follow Fridays (#FFs), hash tags, live tweets, trends topics (TTs), etc.

Twitter also enabled "interactive" TV. So reality TV enables their audience to send comments and opinions via Twitter and if it's live, they



commentators might respond to the messages. Likewise, there are online discussions on live sports, the news and other TV series.



Facebook

was founded on 4th February 2004 by Mark Zuckerberg together with his college classmates and Harvard University students.³

Facebook boasts almost 1 billion active users. One of its particular features is its extreme versatility. Users can choose a pseudonym, create an avatar and post text, links, photos, videos and much more. This information appears instantly and is universally visible. All your 'friends' can see what you publish, wherever they are. This is why we must only express your own opinions, and not those of the organization.



LinkedIn

is a social networking site for professionals and claims 150 million users. It describes itself as a knowledge network, designed to facilitate dialogue between professionals. For its members, it's also a way to manage their online reputation and personal branding.

LinkedIn works on the principle of connections (to contact another professional, you have to know them first, or one of your mutual connections must invite you) and networking, where users build a network of professional contacts.



Weibo

is the Chinese word for "microblog" which provides basic function like message, private message, comment and re-post were made possible in September 2009.⁴



QQ⁵

is another popular social media in China. Same as Weibo, QQ provides news posting over their web sites in China, Hong Kong and Taiwan. QQ is also a kind of instant

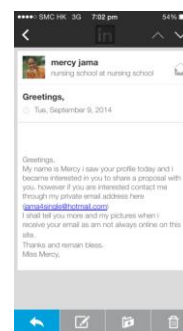
messenger software which can be used at both iOS and Android for messaging and voice transfer.

QQ claims 674 million active users while Weibo claims over 200 million registered users in 2010.⁶

Proper Usage of Social Media

Understanding the aforementioned risks of using social media, the following are recommendations and measures to better protect one's privacy and about how to engage in proper usage of social media:

1. There have been reported incidents that social media sites were compromised leaking out user accounts and passwords⁷. So avoid setting the same password for social media sites and other important personal credentials such as online banking or email. Also, choose carefully the security questions and answers for password resets. Hackers might be able to make educated guesses to bypass the security questions to reset accounts⁸.
2. If you receive a friend request from a person you do not know, do not accept it. If possible, confirm with the friend before adding to your friend's list. Online fake account is easy to be created and pretended to gain information from your profile.



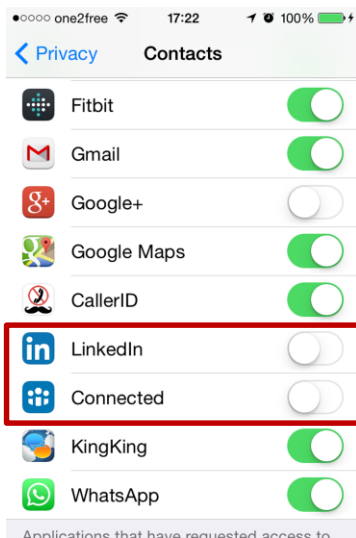
Be careful when handling friend request.

3. Hackers can create fake social media accounts to lure you be connected. Then they will



display fake login page to capture your passwords or even pop up malicious advertisement boxes which can spread computer viruses⁹. To prevent this from happening, always be suspicious when social media such as Facebook asks to log in after you have already logged in. Always check the legitimacy of the web site by inspecting its URL and whether the web site is securely protected by “https” (hypertext Transfer Protocol Secure). To add on a layer of protection, you can configure some social media to send you an email every time someone logs into your account.

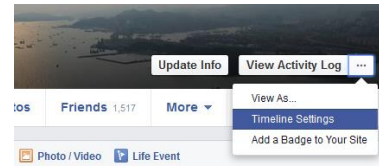
4. Avoid giving permissions to unknown applications to track your geo-location, or collect your personal information such as contact list.



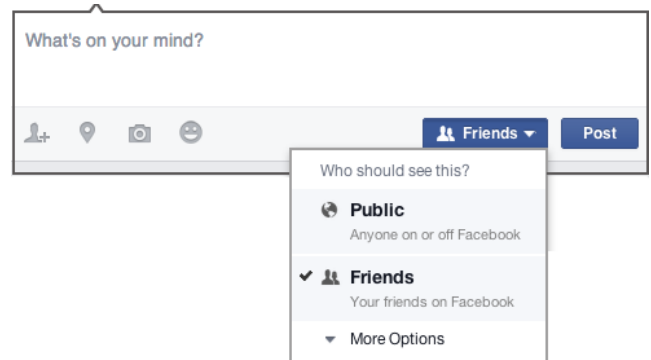
5. Restrict who can view your posting and photos by changing the privacy settings to “only friends” or other restricted groups only. For example in Facebook, through the Timeline Settings, modify your current profile to be viewed by the public or anyone else from your friend list.

To change who can see your tagged pictures and what can be posted in your timeline go to Timeline and Tagging settings and click “Edit”, modify the setting of authority to be tagged

and pictures you posted will be allowed reading by your friends or open to the public.



It is important you have all these privacy settings by default before you post any photo on top of your profile. In addition, people can tag you at any of their pictures which is out of your control, better to have authority pre-set from your profile, you can choose either allow or not allow when someone tag you.



6. Posting any news and articles is another common practice for social media users. However, when you have received news from any source, try to validate the reliability and credibility of the news. Some countries have law enforcement about rumour spreading around the social media (not limited to Facebook) which may have impact to business or reputation of any targeted companies. By clarifying its credibility can protect you from being used by someone who would like to make use of this practice to gain benefits.

‘Do you want your information and messages to be read by your parents and children, also the children of your children forever? Think carefully before post anything onto the Internet.



Nowadays, social media has become part of our lives. The pervasive usage over smartphone will continue to increase our reliance on social media, with more information to be posted and shared.

While enjoying the fun and joy accessing social media, users are reminded to bear the sense of security when dealing with personal privacy and sensitive information.

Social Media and Your Career

Employees have been fired after posting sensitive information or comments that can damage a company's reputation in social networking sites. For example, in 2008 Virgin Atlantic fired thirteen cabin crew members after they criticised the airline's safety standards and referred to passengers as "chavs" on Facebook.

A new survey shows that 71% of Hong Kong hiring managers will check job candidates' Facebook profiles.¹⁰

It is therefore important not to post company sensitive information on social media, and stay vigilant of what you will post and share.

References

1. "Insights & Publications" May 2012. Web. 15 Sept 2014
2. "Why smartphones are the future of social networking?" 8th MAY 2012. Web. 12 Sept 2014
3. "Wikipedia - About Facebook" Web. 12 Sept 2014
4. "Wikipedia – About Weibo" Web. 17 Sept. 2014
5. "Wikipedia – About QQ" Web. 17 Sept 2014
6. "Tencent Vs. Sina: A Look At Who's Winning The Battle For China's Tweets [Infographic]" 5 Aug 2011. Web. 17 Sept 2014
7. "Hackers steal usernames and passwords for TWO MILLION social accounts – and many of the log-ins were as easy as '123'" 5 Dec 2013. Web. 15 Sept 2014
8. "Apple admits guessed iCloud security questions WERE to blame for hacked naked celebrity pictures but insists users photos are safe and its systems have not been compromised" 2 Sept 2014. Web. 15 Sept. 2014
9. "Scammers Are Creating Fake Facebook Accounts Using The Names Of MH17 Victims" 21 Jul 2014. Web. 12 Sept 2014
10. "Use of Facebook May Affect Career Prospects" 24 Mar 2014. Web. 17 Sept 2014

Copyright Statement

All material in this document is, unless otherwise stated, the property of the Joint Universities Computer Centre ("JUCC"). Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.

A single copy of the materials available through this document may be made, solely for personal, non-commercial use. Individuals must preserve any copyright or other notices contained in or associated with them. Users may not distribute such copies to others, whether or not in electronic form, whether or not for a charge or other consideration, without prior written consent of the copyright holder of the materials. Contact information for requests for permission to reproduce or distribute materials available through this document are listed below:

copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC)
c/o Information Technology Services
The University of Hong Kong
Pokfulam Road, Hong Kong