專業資訊保安協會

Social Network Security

Frank K. F. Chow
Vice-Chairperson
Professional Information Security Association (PISA)

How Do We Communicate Today?

- **I can write you a letter by snail mail.**
- **I can write you a letter by email.**
- **I can send you a message via Xbox Live or on my Wii.**
- **I can call you.**
  - From my office phone or mobile device.
  - From my computer running Skype.
- **We can instant message.**
- **We can video conference.**
- **I can be your Facebook friend.**
- **I can access your Myspace page.**
- **I can follow you on Twitter.**
- **I can actually visit you in person?!**

Why Use Social Network?

- It's where the friends are
- Provides a sense of community
- Fun way to stay connected with old friends or make new friends
- Forum for communication (individual/group/mass) and collaboration
- Allows for self-expression and self-representation
- "Crowdsourcing"

2/3rd US households use social networks, twice as many as a year ago

Facebook has over 500 million “active” users, half of which login on any given day, 100 million via their mobile device

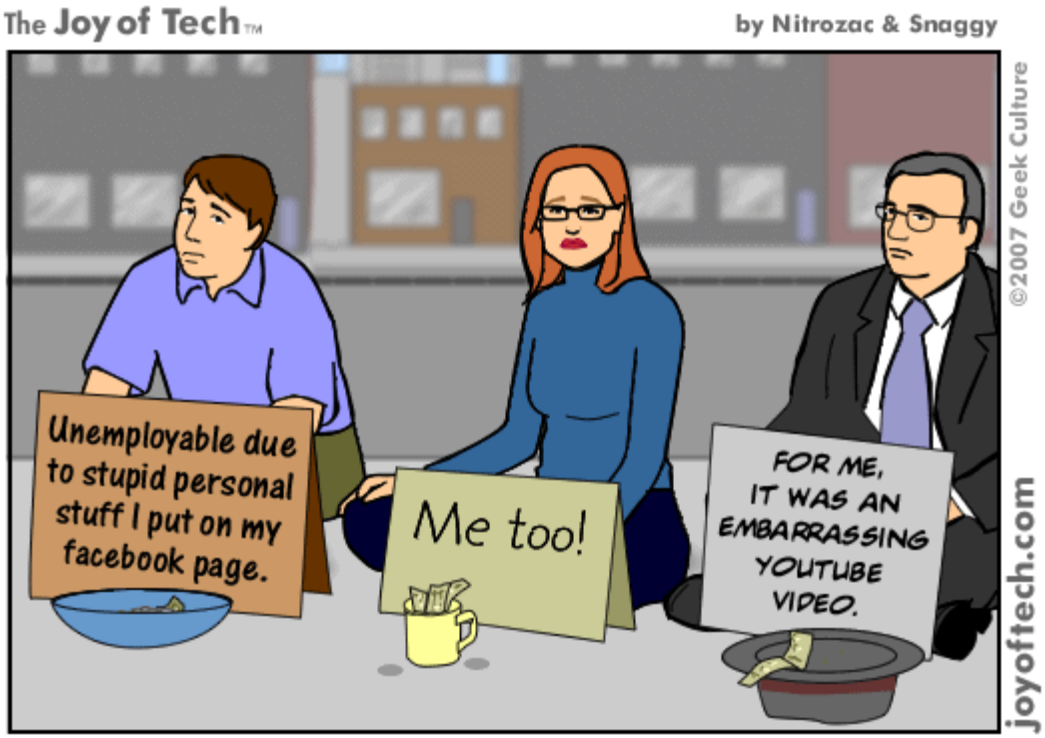
U.S. Facebook users 55 and older grew 922% in 2009 (now ~ 10 million)

What Are The *Security* Risks?

Industry analyst Forrester Research has reported that Web 2.0 applications such as blogs, wikis and social networking sites provide an easy way for data to escape from an organization.

What Are The *Security* Risks?

Can result in social engineering, identity theft, financial fraud, infected computers, stalking, child abuse, sexual predation, lawsuits, mad boyfriend/girlfriend/spouse/parent, unwanted legacy, embarrassment, … job loss



Signs of the social networking times.

How can you protect yourself?

Limit the amount of personal information you post

Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

Be cautious of strangers

The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.

Think carefully about who you allow to become your "friend."

Once you have accepted someone as your friend they will be able to access any information about you (including photographs) that you have marked as viewable by your friends. You can remove friends at any time should you change your mind about someone.

Show "limited friends" a cut-down version of your profile

You can choose to make people 'limited friends' who only have access to a cut-down version of your profile if you wish. This can be useful if you have associates who you do not wish to give full friend status to, or feel uncomfortable sharing personal information with.

Be skeptical

Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.

Remember that the internet is a public resource

Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't withdraw it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.

Evaluate your settings

You can customize your privacy settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

Check privacy policies

Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

Be cautious of third-party applications

Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

Use strong passwords

Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

Do not use same passwords

Do not use the same passwords that you use at work on a social networking site.

Do not use kisok

Never log on to your social network page from public computers such as internet cafés where someone might have installed a key logger and would later get access to your credentials.

Keep software, particularly your web browser, up to date

Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

Use and maintain anti-virus software

Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

Thank You

Frank.chow@pisa.org.hk

www.pisa.org.hk