Social Networking

Wiam Younes
Training and Awareness Coordinator
Information Security Office
Carnegie Mellon University

Information Security Office (ISO) Carnegie Mellon University

What is Social Networking?

Social networking web sites are online "places" where a user can create a profile and build a personal network that connects him or her to other users.

Common Social Networking Sites Used by college Students and Staff

- MySpace
- Facebook
- Orkut
- Hi5
- Faces
- Flicker
- Friendster
- Twitter
- LinkedIn

Features available on a Social Networking Site

- Social networking web sites enable users to share with friends:
  - personal profile
  - list of interests
  - blogs
  - slides
  - music
  - opinions
  - current events
  - school work
  - chatroom conversations
  - videos
  - many other features

THREATS ON A SOCIAL NETWORKING SITE

- No privacy – Information thereafter available in a public domain
- The information and pictures posted by users could haunt them for ever
- Identity theft
- Malware (virus, Trojan horse, worm)
- Spyware
- Phishing
- Cyber stalking
- Copyright infringement
- Legal trouble
- Compromised data

Security Tips

- Install and update your anti-virus and anti-malware with the latest security definitions http://www.cmu.edu/computing/doc/software/index.html
- Keep your system and programs patched and updated

  http://www.cmu.edu/computing/doc/security/index.html
- Make sure your screen name doesn't reveal your real identity
- Choose a complex/unique password for your account. A strong password is at least eight characters long, and consists of letters (capital and small), symbols and numbers

  http://www.cmu.edu/iso/governance/guidelines/password-management.html
- Avoid clicking on links and attachments .
- Avoid clicking on advertisements. Some Maleware hide behind banner ads on legitimate sites
- Follow Carnegie Mellon copyright policy, and Carnegie Mellon Copyright violation guidelines

  http://www.cmu.edu/iso/governance/guidelines/copyright-memo.html

Compromised data

- Compromised Personally Identifiable Information (PII); *PII data refers to name, SSN, D. Licenses, bank accounts*
- Identity Theft- computer intruders intent on stealing your personal information to commit fraud or theft
- Compromised computer; A computer experiencing unexpected and unexplainable

  - Disk activities
  - Performance degradation
  - Repeated login failure or connections to unfamiliar services
  - Third party complaint of a suspicious activity

Compromised machine or data?

Responding to a Compromised/Stolen Computer

http://www.cmu.edu/iso/governance/procedures/compromised-computer.html

Compromised - Reasonable suspicion of unauthorized interactive access

1. Disconnect From Network
2. Do NOT Turn Off
3. Do NOT Use/Modify
4. Contact ISO & Dept Admin
5. Preserve External Backups/Logs
6. Produce Backups/Logs/Machine ASAP For Investigation

Also report stolen computers

ISO Breach Handling Process

The ISO:

1. Confirm compromise, notifiable data, and likelihood of data breach (stolen laptop = data breach)
2. If data breach – proceed to notification

The ISO, the organization, & General Counsel's Office:

3. Identify population and locate current contact info via alumni records
4. Draft & send notification letter and interface w/ law enforcement and consumer reporting agencies as required
5. Operate call center and respond to legal action

rity Office(ISO)

Stolen Identity

If you suspect that you are a victim of identity theft;
http://www.cmu.edu/iso/aware/idtheft/notify/index.html

1. Report identity theft to your local police department
2. Contact the fraud hotline at the Social Security Administration (SSA), if your social security number was stolen
3. Contact the fraud department of the three major credit bureaus
   - Equifax
   - Experian
   - Trans Union
4. Contact your creditors or bank when you suspect that your credit card, debit card or bank account is compromised.

How to find and handle Sensitive data

1. Know what data is stored on your personal computer

Run identityfinder

http://www.cmu.edu/computing/doc/security/identity/intro.html

Training material and video is available at

http://www.cmu.edu/iso/aware/id-finder/index.html

Safety tips

- Read the privacy policy of the website carefully. Make sure your information is not shared with a third party or sold to marketing entities
- Set appropriate privacy and security defaults
- Consider restricting access to your page to a few of your friends. You don’t want people you write on your wall what you don’t support (know? Trust?)
- Limit the amount of personal information posted on your page
- Avoid posting information you consider private
- Only accept “friend” requests from people you know directly
- Restrict or delete “public search listing” access
- Be skeptical of accepting any online information as truth

Facebook privacy and security guide

Social Media Security provides the following instruction to privacy and security settings on Facebook via the following link:

http://socialmediasecurity.com/wp-content/uploads/2009/07/Facebook_Privacy_and_Security_Guide.pdf

ISO RESOURCES

Resources:

- Identity Theft
  http://www.cmu.edu/iso/aware/idtheft/index.html
- Viruses, Worms and Breakins
  http://www.cmu.edu/iso/aware/be-aware/virus.html
- Spyware
  http://www.cmu.edu/iso/aware/be-aware/spyware.html
- Carnegie Mellon Copyright Policy
  http://www.cmu.edu/policies/documents/Copyright.html
- Copyright infringement legal notices
  http://www.cmu.edu/iso/aware/P2P/notice.html
- Guidelines for password management
  http://www.cmu.edu/iso/governance/guidelines/password-management.html
- Responding to a Compromised/Stolen Computer
  http://www.cmu.edu/iso/governance/procedures/compromised-computer.html
- Secure Computing
  http://www.cmu.edu/iso/aware/secure/index.html
- Computing Services, Security
  http://www.cmu.edu/computing/doc/security/index.html

References

- Anderson Analytics – Facebook ranked NO.1 among college students

  http://www.marketingcharts.com/interactive/college-students-facebook-top-site-social-networking-really-hot-1914/
- Forty-Five percent of Employers use Social Networking sites to Research Job Candidates, according to CareerBuilder Survey in 2009

  http://www.marketwatch.com/story/forty-five-percent-of-employers-use-social-networking-sites-to-research-job-candidates-careerbuilder-survey-finds-2009-08-19?siteid=nbsh
- Cyber Stalking – A detailed Look Inside the Behaviors of Cyber Criminals

  http://www.bukisa.com/articles/147295_cyber-stalking-a-detailed-look-inside-the-behaviors-of-cyber-criminals
- 2009 Study from Ohio State shows college students who use Facebook may earn lower GPAs

  http://www.collegenews.com/index.php?/article/study_shows_that_college_students_who_use_facebook_gets_lower_gpas_041420098383/
- US- CERT - Reviewing End-User License Agreement

  http://www.uscert.gov/cas/tips/ST05-005.html

Information Security Office (ISO) Carnegie Mellon University

INFORMATION SECURITY OFFICE (ISO)

If you have a security related question, please do not hesitate to contact the ISO at:

iso@andrew.cmu.edu

Office: (412) 268-2044

Support: (412) 268-4357

Information Security Office (ISO) Carnegie Mellon University