SOCIAL NETWORKING: HOW SECURE IS YOUR ORGANIZATION

Dr. Johnson Mwebaze
Uganda Technology & Management University
In this talk

Overview & introduction
Threats
Defense Measures
The value of social Networking lies not just in the content provided (which is group-specific) but in its replication in electronic form of the web of human relationships and trust connections.
Social Media - includes

THERE'S A LOT…

pick what makes sense for your objectives
Some Statistics & Facts

Facebook maintains its top spot at over 60% penetration of all internet users globally with YouTube at around 44%, Google+ (43%) and Twitter at 35%.

The fastest growing demographic on Twitter is the 55–64 year age bracket.

Social Media has overtaken porn as the #1 activity on the web.

25% of Facebook users don’t bother with privacy settings.

Over 1 million websites have integrated with Facebook.

Conclusion: Social media isn’t the intern’s job anymore. A successful approach will require some high-level strategy.
### Social Media Perspectives

These perspectives cover the Social Media interactions of an organization.

<table>
<thead>
<tr>
<th>Perspective</th>
<th>Top Risk Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization-Internal</strong></td>
<td>Technology Adoption</td>
</tr>
<tr>
<td>• Hosted on organization-owned or controlled technology</td>
<td>Lack of Collaboration and Sharing</td>
</tr>
<tr>
<td>• Restricted to organization employees only (in some special cases to clients and vendors)</td>
<td></td>
</tr>
<tr>
<td><strong>Organization-Public</strong></td>
<td>Security and Privacy</td>
</tr>
<tr>
<td>• Hosted on organization-owned technology (like a CEO blog on organization's website) or is hosted by an external provider on their technology</td>
<td>Brand and Reputation</td>
</tr>
<tr>
<td>• Open to public</td>
<td>Regulatory and Legal</td>
</tr>
<tr>
<td>• Sponsored by the organization or one of its business units in accordance with the organization policy</td>
<td>Information leakage</td>
</tr>
<tr>
<td><strong>Personal</strong></td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>• Hosted by an external provider on their technology</td>
<td>Productivity loss</td>
</tr>
<tr>
<td>• Open to public</td>
<td></td>
</tr>
<tr>
<td>• Not sponsored by the organization</td>
<td></td>
</tr>
</tbody>
</table>
# Social Media Perspectives – Organizational and Personal

<table>
<thead>
<tr>
<th>Anticipated Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal &amp; Regulatory Compliance</strong></td>
</tr>
<tr>
<td>• Disclosure of confidential information</td>
</tr>
<tr>
<td>• Violation of copyright laws</td>
</tr>
<tr>
<td>• Protection of intellectual property rights</td>
</tr>
<tr>
<td>• Legal and financial ramifications for noncompliance with industry regulations</td>
</tr>
<tr>
<td><strong>Security &amp; Privacy</strong></td>
</tr>
<tr>
<td>• Identity theft, Social engineering</td>
</tr>
<tr>
<td>• Ability to retain and log social media communication; data retention</td>
</tr>
<tr>
<td>• Technical exploits: Malware, Viruses/Worms, Flash Vulnerabilities, XML injection</td>
</tr>
<tr>
<td><strong>Brand and reputation damage</strong></td>
</tr>
<tr>
<td>• Posting unfavorable or confidential information on a public site</td>
</tr>
<tr>
<td>• Unclear behavioral expectation of end users to use social media</td>
</tr>
<tr>
<td>• Defamation, Copyright infringement</td>
</tr>
<tr>
<td><strong>Productivity loss</strong></td>
</tr>
<tr>
<td>• Use of social media can be a distraction i.e. employees accessing non-work related social media sites</td>
</tr>
<tr>
<td>• Acceptable use of social media</td>
</tr>
</tbody>
</table>
Social Media Risk Landscape

Social Media usage presents behavioral, application and technology related risks. The risk landscape is vast and continuously evolving.
Threats:
... they are real:

Facebook Scams You Need To Know About: The 9 Most Common Hacks And Attacks
The Huffington Post | Catharine Smith tw | First Posted: 05/22/11 04:25 PM ET | Updated: 07/22/11 06:12 AM ET

LinkedIn's Password Breach Draws FBI's Attention
LinkedIn said it is “in contact with the FBI” concerning this week’s security breach that led to Internet postings of 6.5 million hacked passwords for members’ accounts.

Facebook users hit by 'Koobface' virus that seeks out credit card numbers
By DAILY MAIL REPORTER

WARNING: Facebook Malware Attack Behind Distracting Beach Babes Video

Facebook Clickjacking Worm Persists
Spread via status messages, there's no mention of the 'likejacking' attack on Facebook's security page.

By Mathew J. Schwartz, InformationWeek
June 3, 2010
Linked In

Additionally, you grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicensable, fully paid up and royalty-free right to use, copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to LinkedIn, including but not limited to any user generated content, ideas, concepts, techniques or data to the services, you submit to LinkedIn, without any further consent, notice and/or compensation to you or to any third parties. Any information you submit to us is at your own risk of loss.

Facebook

“You hereby grant Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, translate, excerpt, adapt, create derivative works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof subject only to your privacy settings or (ii) enable a user to Post, including by offering a Share Link on your website and (b) to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof. You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.”
Malware Distribution

Malware/malicious software

Malicious ads

Click Jacking or "likejacking"

Wall posts, inbox or chat messages with malicious links from "Friends" (hijacked user account)
URL Shorteners

bit.ly, TinyUrl, ReadThisURL, NotLong

Hides the true destination URL – no way to tell where you’re going until you click!

http://www.hacker.com/badsite?%20infect-your-pc.html

is now


DANGER! ENTER AT YOUR OWN RISK! BEWARE!
Jessica would like to be your friend on hi5!

I set up a hi5 profile and I want to add you as a friend so we can share pictures and start building our network. First see your invitation card I attached! Once you join, you will have a chance to create a profile, share pictures, and find friends.

Invitation Card.zip
Many spammers have sought to capitalize on the exponential growth of social networks and the free traffic they provide; How?

- The use of specialized social networks spamming software such as FriendBot

- Sending of notes typically including embedded links to pornographic or other product sites designed to sell something

- Friend invitations, using an attractive profile which is likely to persuade someone to accept the invitation.

- Stealing members’ passwords to insert and promote their offers on another profile

RISKS: Traffic Overload, phishing & diversion, fake profiles, etc.

Spam

Friday 5th October 2007

Man jailed for adding wife to Facebook friends

10:06AM, Friday 5th October 2007

A husband who was banned from contacting his wife following their split was jailed after "accidentally" sending her a message on Facebook.

Dylan Osborn was ordered by the courts not to contact his ex-partner, Claire Tarbox, after barraging her with phonecalls and text messages after they broke up, reports the The Daily Telegraph.

However, after joining Facebook to view the wedding album of a friend, the social networking site automatically sent a "friend request" to every name on his email list, including that of Tarbox.

Though Osborn claimed to have no knowledge of the request, his ex-partner reported him to the police who subsequently arrested him for violating the conditions of his bail.
CBIR – Content Based image retrieval

was originally developed for digital forensics.

CBIR allows linking of location data through the recognition of common objects in images.

CBIR opens up the possibility of deducing location data from apparently anonymous profiles containing images of users’ homes/offices/work yards.

This can lead to stalking, unwanted marketing, blackmail and all the other threats associated with unwanted disclosure of location data.
Usage of face recognition allows the linking of image instances (and the accompanying information) across services and websites. Both CBIR and face recognition are part of a broader threat posed by so-called 'mashups', which link data between independently provided web services to provide previously unforeseen inferences including highly personal information. This enables connecting pseudo-anonymous dating profile with an identified corporate website profile.

Data Mining Tools – Face Recognition

Does not seem to work very well....
Corporate Espionage

Use social engineering used to access sensitive enterprise data

- not by using technology but by using the employees themselves.
- data is often acquired subtly and is gathered gradually piece by piece.

Social media platforms encourage a dangerous level of assumed trust.

- Users are willing to share personal information –
- Easy to tell a new friend about your company’s secret new project
- it's a short step to telling your new friend about your company's secret project.
Corporate Espionage - Example

Possible to lists employees currently or previously working at Barclays Bank,

Could be used for social engineering attack on an enterprise.
How Data Leaks: Loose lips

Virgin Atlantic flight attendants who mentioned engines replaced 4 times/year, cabins with cockroaches
How Data Leaks: apps

Installation gives the developers rights to look at your profile and overrides your privacy settings!
Isn’t my privacy settings enough?

Identity 'at risk' on Facebook

By Spencer Kelly
Presenter, BBC Click

Personal details of Facebook users could potentially be stolen, the BBC technology programme Click has found.

The popular social networking site allows users to add a variety of applications to their profile.

But a malicious program, masquerading as a harmless application, could potentially harvest personal data.

Facebook says users should exercise caution when adding applications. Any programs which violate their terms will be removed, the network said.

Stealing details

Facebook is the darling of the moment, allowing friends to stay in touch, post photos, and share fun little games and quizzes. And it also lets you keep your details private from the rest of the world. Or at least that is the implication.
Digital Dossier Aggregation

Profiles on social networks can be downloaded and stored over time and incrementally, creating a digital dossier of personal data:

- Data can be used to track and highlight changes (e.g. list of JOBs/girlfriends over time).
- Information can become embarrassing, damaging,
- Blackmailing scheme to embarrass the profile holder
- The nature of staff that you employ is known, which can lead to integrity issues.

In a recent case, the current Miss New Jersey was threatened with publication of images taken from her profile if she would not give up her crown.
Secondary Data Collection

Social Networks are not mere collection of profiles but a one-stop communication hub for messaging services, interest groups, video content and more.

Network operators and application providers can now gather unprecedented amounts of secondary personal information on their users.

- it can also be used for targeting (e.g. advertising), discrimination (e.g. price discrimination) or the transfer of data to third parties through resale.
Moreover, in general there is ambiguity as to whether information will be deleted upon account closure.

Upon ‘deactivating’ an account, users of some providers such as Facebook receive an e-mail telling them how to ‘reactivate’ their account – implying that a copy is kept of personal data.

Damaging comments cannot be removed, increasing the ‘digital dossier’ effect.
Cross Site Scripting (XSS)

Victim’s browsers is induced to execute malicious code

In some social media, users can post HTML within their own profiles and message-boards.

In addition, a heavy reliance on message posting and viral marketing means Social Networks viruses spread extremely quickly.

E.g. the SAMY ViRUS spread to over one million users within just 20 hours on MySpace

Among the effects of such vulnerabilities are:

- Account compromise
- Denial of service (SAMY forced MySpace to shut down its site) and associated loss of reputation
- Cause Victim’s computer to launch an attack on their corporate networks.
- Unsolicited content may also be spread to e-mail and IM traffic (SNSs generate e-mail and IM messages).
Infiltration of networks leading to information leakage

Social and commercial pressure to get as many friends as possible means

- there is often a tendency to accept friend requests without checking their authenticity or suitability
- Become someone's 'friend' under false pretenses

Experiment by SOHOS, created a pseudo-profile and sent out 200 request

- 87 of the 200 users contacted responded to Freddi, with 82 leaking personal information (41% of those approached)
- 72% of respondents divulged one or more e-mail address
- 84% of respondents listed their full date of birth [52].
Fake profiles are created in the name of well known personalities or brands or in order to slander people who are well known within a particular network of friends. Fake profiles can be used for malicious purposes such as defamation, etc. Such profiles can be used to lure unsuspecting users into divulging information which can be used for phishing attacks, marketing under false pretences, profile squatting and reputation slander through ID theft.

**Summary:** Chinese spies created a fake Facebook profile of U.S. Navy admiral James Stavridis, friended various NATO officials, and gained access to their personal data. The fake profile has since been taken down.
Human Error: Employee Greatest Risk

**Why?**

- Because they *introduce* the problems by showing poor judgment,
- clicking things they shouldn’t and
- generally being lazy about applications that unload viruses, spyware and malware.

- Employees can also unwittingly overshare confidential information, which is gold in the wrong hands.
  - Even piecemeal information dropped here and there can be stitched together and used by a good hacker to bring your company to its knees.
Information “shelf life”

Common sense: it’s very difficult to delete information after it’s been posted online.

Indiscreet information can adversely affect any organization.

Twitter gave its entire archive to Library of Congress in 2010.
Information Privacy

Information posted on Social media is generally public

- “I’ll be on vacation” post plus geolocation invites burglars, i.e., “Please visit my house – u cld find usefull company information”

Indiscreet posts can lead to nasty consequences

Don’t drink and Facebook. This should go without saying, but sometimes (at least) our ability to communicate is impaired by drinking. Drinking and e-mailing (or social networking) just don’t go together. You’re better off not logging in.
Social Network Aggregators

Social Aggregators integrate data from various social networks into a single web application.

They multiply the vulnerability of accounts by giving read/write access to several social networks accounts based on a single weak username/password authentication.

Social Aggregators also carry the risk of increasing the potential for attackers to mine data across sites since many offer cross-social network search features.

Many of the risks are the same as with any kind of authentication compromise
Best practices, how to protect your brand, organization, etc
Guarding Your self

Clear corporate policies on social network usage inside AND out of the office. E.g.

- Hours where SN usage is allowed enforced by firewall.
- Clearly define which corporate data is not permitted on social networks.
- Recommend privacy settings to be used on networks
- Conduct awareness-raising campaigns

Organizations must conduct proper training for employees

A social media initiative needs a coordinator and champion. And that means a social media manager.
Defense Measures (1)

“Common sense” measures:

- Use strong, unique passwords
- Provide minimal personal information: avoid entering birthdate, address, etc.
- Review privacy settings, set them to “maximum privacy”
  - “Friends of friends” includes far more people than “friends only”
- Exercise discretion about posted material:
  - Pictures, videos, etc.
  - Opinions on controversial issues
  - Anything involving coworkers, bosses, classmates, professors
  - Anything related to employer (unless authorized to do so)
- Be wary of 3rd party apps, ads, etc. (P.T. Barnum’s quote)
- Common sense: think before you click
Defense Measures (2)

More advice:
- “If it sounds too good to be true, it probably is”
- Use browser security tools for protection:
  - Anti-phishing filters (IE, Firefox)
  - Web of Trust (crowdsourced website trust)
  - AdBlock/NoScript/Do Not Track Plus
- Organizational reputation management:
  - Search for yourself online, look at the results…
  - Google Alerts: emails sent daily to you about results for any search query (free), e.g., your name
Defense Measures (4)

Organizational defense is more complicated:

- Monitoring employees’ use of social networks
- Monitoring org’s name, logo appearance on social Networks
- Responding to attacks on org. in a timely manner

Encompasses all parts of an org., not just IT dept!

This usually entails: [1]

- Crafting social media policy, disseminating to employees
- Hiring/training staff to manage org. presence on social networks (with management oversight)
- Monitoring and reporting employee use of social media
  ...

Example tools:

- Google Alerts (emails as “search query” appears online)
- HowSociable (shows mention of org. name/brand on Social Networks)
- SocialGO (create your org.’s own social network)
- Tech/404 Data Loss Calculator (self-explanatory)
- Chartbeat (monitor customer engagement on website)
- EventTracker (monitors employee activity)
- Many more…
Questions?
REFERENCES (1)


REFERENCES (2)


17. https://twitter.com/BPglobalPR

