



The Information Security Implications of Social Networking

ACORD/LOMA Systems Forum

May 2009

**Steven Attias, CISSP, CISM, FLMI
New York Life**

The Company You Keep®



Agenda

Background

Challenges

Threats

Hacks

Mitigations

Questions



The Premise For Social Networking

The fact that you are here, I assume means you have some notion of Social Networking or Social Media.

What is it about this phenomenon that allow people to share the most intimate facts about themselves in a public forum that they would NEVER reveal in a bar or at a cocktail party?

Whatever it is, Gen Y people seem to be quite willing to do so, expect their peers to do the same, and thus this has tremendous impact on the way companies deal with these people, as employees and as customers!



Some Social Networking Sites

Top 25 Social Networks Re-Rank

(Ranked by Monthly Visits, Jan '09)



Rank	Site	UV	Monthly Visits	Previous Rank
1	facebook.com	68,557,534	1,191,373,339	2
2	myspace.com	58,555,800	810,153,536	1
3	twitter.com	5,979,052	54,218,731	22
4	fixster.com	7,645,423	53,389,974	16
5	linkedin.com	11,274,160	42,744,438	9
6	tagged.com	4,448,915	39,630,927	10
7	classmates.com	17,296,524	35,219,210	3
8	myyearbook.com	3,312,898	33,121,821	4
9	livejournal.com	4,720,720	25,221,354	6
10	imeem.com	9,047,491	22,993,608	13
11	reunion.com	13,704,990	20,278,100	11
12	ning.com	5,673,549	19,511,682	23
13	blackplanet.com	1,530,329	10,173,342	7
14	bebo.com	2,997,929	9,849,137	5
15	hi5.com	2,398,323	9,416,265	8
16	yuku.com	1,317,551	9,358,966	21
17	cafemom.com	1,647,336	8,586,261	19
18	friendster.com	1,568,439	7,279,050	14
19	xanga.com	1,831,376	7,009,577	20
20	360.yahoo.com	1,499,057	5,199,702	12
21	orkut.com	494,464	5,081,235	15
22	urbanchat.com	329,041	2,961,250	24
23	fubar.com	452,090	2,170,315	17
24	asiantown.net	81,245	1,118,245	25
25	tickle.com	96,155	109,492	18



Social Network Impacts

Social Network Sites (SNS) offer a lot of good

Marketing, sales, business alliances

Social outlet, peer connections, collaboration

BUT – The FACT is they clearly offer the foundation for the unscrupulous to take advantage, via:

Malware deployment

ID Theft

Personal harassment (and worse)

Spamming



The Challenges

With new fertile ground for “bad activities”, is it a wonder that Companies want to ban/block these sites?

- Lost Productivity
 - Facebook vs. Company deployed VPN & Blackberry?
 - Management issue, not security
- Security Concerns (more surface to attack)
 - Malware
 - Data loss
- Compliance Concerns



The Security Threats

The popularity of SNS' such as Facebook, LinkedIn and MySpace means that they will (have) become a target for attackers. It can be easier than attacking PCs.

Actions to protect the information requires, user, enterprise and SNS provider actions.

Threats to date include:

- Loss of Company Data

- Identity Theft

- Brand Damage

- Harassment, Discrimination, Hate Crimes



Recent “Hack” #1

Computerworld Headline: Fake LinkedIn profiles promise prurient pics, send patsies malware instead Expect more attacks to come from social networking services, says security expert

January 7, 2009 (Computerworld) Hackers have seeded LinkedIn Corp.'s business networking service with bogus celebrity profiles that link to malicious sites serving up attack code, a security researcher said today.

Unlike Twitter, which had nearly three-dozen legitimate accounts hijacked on Monday, LinkedIn was not compromised. Instead, criminals used the service to create phony profiles, gave them celebrities' names and slapped on the word "nude" to further entice users. The celebrities named included singer Beyoncé and actresses Christina Ricci, Kirsten Dunst and Kate Hudson.



Recent “Hack” #2

Headline: Facebook hit by phishing attack

April 30, 2009: A scam that tries to steal people's Facebook password details – using a website that mimics Facebook's login page – is spreading rapidly through the social networking site.

The scam's emergence comes as a report shows that Facebook was the seventh most popular target of such "phishing" scams in March – although it is some distance behind PayPal and eBay, the two most popular targets, and banks such as Bank of America, HSBC and Alliance Bank.



Attacks on Social Networking

Social Engineering



Social Networks



Social Engineering

The act of manipulating people into performing actions or divulging confidential information.

The term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.

Kaspersky Labs found that last year 90% of all malware was carried via social engineering attacks.



Why Attack Social Networking Sites?

“Social networking sites are meant to get as many users in one place as possible on one platform, and for attackers there's a lot of return-on-investment in going after them, this creates the climate as a perfect storm of social engineering and bad programming.” – Shawn Moyer

Implanting Malware via this approach – much easier than hacking code, looking for vulnerabilities.

Purpose is financial gain, by:

- Directly controlling the endpoint to use as spam or malware bot
- Access personal information (more friends addresses, Account information, Game Account access)



7 Deadliest SNS Hacks

- 1) Impersonation and targeted personal attacks
- 2) Spam and “Bot” infections
- 3) Weaponized social networking applications
- 4) Crossover of personal to professional online presence
- 5) Web application attacks (XSS, CSRF)
- 6) Identity theft
- 7) Corporate espionage

From DarkReading 8/26/2008



Impersonation

The very nature of SNS' which people join to share information make this easy.

Putting yourself visibly “out there”, leaves you open for attack. Or someone else can put you out there.

Posting your every whereabouts and activities (Twitter) can lead to all sorts of physical problems – including at the workplace.

There's enough information online that someone can create your profile (or one like it) on an SNS. Now, do you really know who you just befriended? Did you just exchange a quip with your boss, or have you divulged a clue to company secret?



Spam and Bot Infections

So now you have access to your “friend’s” phony site. Why wouldn’t you click on that link for the video of their last speech, vacation, party? Next step will be downloaded malware silently on your PC!

This allows rapid spreading of malware across the SNS. With 6 degrees of separation, you’ll soon be infecting (or infected by) Kevin Bacon!



Weaponized Applications

So installing an application or plug-in in your Browser, No Biggie, right?

You trust every piece of active code sent by the SNS? It's third parties? With their flawed (Facebook) API? (See "Secret Crush")

These applications can access (and have) more private information that they should have (more than they needed).

The more the client system (and its human driver) trust the applications, the more opportunity to do harm.



Personal Meets Professional

Even if you keep separate accounts, there is likely outcome that personal stuff will bleed into the professional profile and vice versa.

Limiting profiles to bare minimum, and using the security settings often present (and largely ignored) can reduce the risk.

This is especially important for staff charged with maintaining the Company's SNS profiles. These users must be registered with their own profiles. Therefore they could becoming victim (targets) of social engineering or phishing attacks, or even account hijacking.



Web Application Security Attacks

Common application coding vulnerabilities such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) can be exploited.

XSS is a server side attack, which allows malicious code to be injected into Web applications and then users viewing that page can be infected.

CSRF, a client side attack, its use is on the rise, it coerces the client to infect pages on web sites it is already authorized to access.

The Browser is the best place for malware to attack. Again, these attacks are not unique to SNS', similar attacks have infected Google, eBay and other "reputable" sites.



Identity Theft

Giving away several little pieces of your profile (name, date of birth, address) allows malicious users to cull this information and use it to guess passwords (hijack accounts) or impersonate someone.

Since people often use the same password across many systems, its possible for someone to then turnaround an attempt to crack the users' Company system.

Guidance: Avoid using personal information. Why use your *real* birth date, you your mothers *real* maiden name? Your real friends already know your personal information, why give it to total strangers?

The 6 degrees of separation rule applies here too.



Corporate Espionage

With so much personal information available in SNS' (and other web places), a spear-phishing attack could trick someone into divulging information.

That message from Human Resources posted to your LinkedIn account asking you to sign into this new Company application, could easily be harvesting your login credentials!

Network access is the key to Company secrets!



Mitigate Risks via: Internal “Facebook”

Some business have has success creating an internal solutions, in other places, it did not take hold.

Depending on the organization and the purpose, this may offer some of the benefits of SNS, while reducing risks.

However, for external Company activities (Marketing, Sales, Recruiting) it clearly is a non-starter.

For social networking and collaboration – the “digital natives” will probably not devote their time here – not when they can extend their network far beyond company “e-walls”. In college, they used FB to meet across universities, not just in their home school.



Mitigate Risks: Is Blocking Really Feasible?

Technically – probably, using URL filtering

- But that's in the office, how to you block from home?
- Blocking reduces risk of malware, but does little to protect you from data leakage, ID theft or corporate espionage

Socially – maybe, if you are the FBI, DOD, etc.

Blocking is often used by management to stop the “loss of productivity”, and security people are only too happy to oblige!

But ---



Mitigate Risks: Is Blocking Really Feasible?

- Do you block the use of email?
- Do you block access to company phones? Personal cell phones?
- Do you block all Internet Access?
- Do you expect to hire employees under the age of 30?
- ***All the security issues*** associated with SNS' already exist and we deal with them everyday (yes, attack surface area has increased)

Then:

- Best we learn how to reduce risk to a reasonable level!



Mitigating Risks

If Blocking (long term) isn't the answer, what do we do?

This is a people-tool, so technical controls will always be limited. They can help stop mistakes, they generally will not stop malicious behavior. This is NOT an SNS issue.

As stated previously, all the threats exist today in some form, outside of SNS'.

→ Governance and Awareness



Mitigate Risks via: Policy, Awareness and Governance

Where do we always start with reducing risk – with the people! Policy comes first.

Develop (or enhance) policy regarding use of company information externally.

Provide awareness of the risks, no different than:

- Anti-phishing campaigns
- Use of strong passwords
- Don't click on attachments from unexpected emails
- Make staff accountable for their actions which affect the Company

Provide guidance on safe usage of SNS'

Governance included monitoring – both of any Company sponsored presence, as well as looking for employee sites



Mitigate Risks via Technical Controls

Use controls already at your disposal – but recognize that they are usually limited to activity coming from your network!

Web Security Gateways – can filter both ways, outbound access as well as inbound content. These can prevent malicious code hosted on SNS's from entering your network.

Endpoint security – AV, Anti-spam, Anti-spyware, Intrusion Detection, Personal Firewalls. This second layer provides additional protection, as well as reducing risk from mobile machines which connect to other networks.

Content filtering tools – examine the content leaving your network for personal information, “internal use only”, etc.



Remember – Exposure is forever!

Once exposed, information cannot be recovered and made confidential again.

As a result, prevention of data loss is a priority.

On a personal level, the same applies. Once you disclose a personal item (say an ill-advised picture), it may be captured and replayed throughout your career!!



Questions

