



Proceed with Caution...*Social Networking Risk Management Strategies*

Manage It.
Measure It.
Expect It.

Matt Riley, CIO, Gladiator Technology, ProfitStars



Social Media Communication

twitter



- Found here: <http://socialmediaanswers.com/niche-social-networking-sites/>



Financial Institutions and Social Media

- **Collaboration...**
- **Access...**
- **Trust...**
- **Relationships...**
- **Community...**



Financial Institutions and Social Media

- **Six in 10 financial institutions consider themselves to be either novices or beginners at social media**
- **90% of FIs say they expect to have dedicated budgets for social media efforts by 2012, with one-third anticipating the creation of a new budget**
- **30% of bankers say their IT organizations are involved in managing the firm's social media efforts**

* (Nov. 2010 - Aite Group, LLC Study) Social Media at the Starting Blocks: A Look at Financial Institutions in Europe and the United States



Social Media

Aspects of Social Media:

- **Personal Use**

External and Internal:

Profiles, connect with friends, post reviews and ratings, blogging

- **Business Use**

Internal and External:

Research

Informational

links to community news

Promotions

Finance tips

Advertising rates

****Communication with customers**





Consider the Following First!

- **Objectives**
- **Risk/Reward**
- **Appropriate Controls/Standards**
- **Measuring/Monitoring tools**





The Threat Landscape

- **Threat categories**
- **What's the goal?**
- **What makes social networks different?**
- **Threat details**
- **What can you do about it?**

•From <http://www.zdnetasia.com/top-5-social-networking-business-threats-62060912.htm>



Technical Threats

4 Categories*

- **Malware**
- **Spam**
- **Social Engineering/Phishing**
- **Corporate Data Leakage**

1 Goal: To Make Money

- **Sending spam**
- **Stealing confidential, valuable information**
- **Stealing money directly**

•From <http://www.zdnetasia.com/top-5-social-networking-business-threats-62060912.htm>



What's Different?

- **These are the same threats for web browsing**
- **Why are users more vulnerable?**
- **Trust!**
 - **Users trust social network “friends”**
 - **Seen as an authenticated medium**
 - **Fake profile pages are more likely to be trusted**
- **Lots of personal information**
- **Increased Attack Surface**



The Malware Threat

- **Malware Targeting Social Media Accounts**
 - Password Stealers
 - Mass Mailers/Spammers
- **Malware Delivered Over Social Media**
 - Exploiting trust
 - Messages from strangers or friends
 - Delivered using URL Shortening Services
 - <http://tinyurl.com/ye6aqfv>
 - Phony Applications built for Social Networking (Facebook Apps)
 - Dislike Button
 - App to see who has been viewing your profile
 - Free Farm Cash!



Social Networking



DISLIKE BUTTON



 You dislike this.

This will add a "Dislike" feature to your facebook. You will have the ability to dislike any of your friends statuses. Simply click the install button below to use the application.

Downloads: **765,629**
Updated: April 23, 2010
Rating: ★★★★★

INSTALL

 **Thomas Moquet** voici la nouvelle version de Facebook Dislike :
5 hours ago · Comment · Like · Undislike

 Marion Carrin likes this.

 Cédric Tissot, Philippe Court, Maxime Le H., Pascal Filipovicz, Thomas Moquet, Paul Dupuis, Ludovic Savignan, Manon Aubertin and Thomas Moquet dislike this.

 View all 16 comments

Social Networking



facebook Home

FARMVILLE
by zynga

Congratulations,
You just won 310 farm cash and a special guide to teach you how to use them wisely!

 310  ~~\$50.00 USD~~ **Free Bonus**

Select package: 310 Farm Cash (Free Bonus)

[Continue >](#)

We tell you exactly what to do with the farm cash and how to become the best player in Farmville!

-  **Best Tips and Tricks**
Learn the latest tips and tricks for a good farm.
-  **Hacks and Cheats**
What hacks and cheats actually DO work.
-  **Stay up to date**
Be sure to get your hands on the latest farmville items.

310 FV Free Cash Christmas Bonus [Zynga Official] - Report/contact this application - English (UK) [About](#) - [Advertising](#) - Dev



Social Networking

Request for permission

310 FV Free Cash Christmas Bonus [Zynga Official] is requesting permission to do the following:

	<p>Access my basic information Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.</p>		
	<p>Send me email 310 FV Free Cash Christmas Bonus [Zynga Official] may email me directly at</p>		<p>310 FV Free Cash Christmas Bonus [Zynga Official]</p>



The Malware Threat

- **Firesheep**

- Free add-on for the Firefox Browser
- Automated Facebook password stealer
- Steals credentials over wireless networks
- **Don't use open wireless connections**
 - Use a VPN tunnel to secure connection

- <http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=227900742&cid=RSSfeed>
- <http://www.networkworld.com/community/blog/firesheep-firestorm>



The Spam Threat

- **Another Inbox to check**
 - No spam/antivirus filter
 - Checking messages while at work
 - “Hey, check out this link of me in a funny video!”
- **Sending spam as a friend**
 - Spammers compromise accounts and send messages to all friends
 - Can use URL shortening services
- **Messages can deliver malware**



The Social Engineering Threat

- **Information Gathering**
 - Employee Profiling
 - Customer Profiling
- **Targeted attacks, combining information from multiple sites**
- **Combines well with other social engineering**
 - SMS Phishing
 - Email phishing
 - Links to fake websites



Social Engineering Examples

- **Financial Institution Fan Page (Facebook)**
 - Shows who is a fan of the institution
 - A good place to target your customers
 - If posting is allowed, can post targeted malware
- **Fake FI Fan Page**
 - If you don't create one, they will!
 - Masquerades as official website
 - Links to malware/phishing



The Data Leakage Threat

- **Employees are accessing these sites at work and at home on corporate laptops**
- **Hard to monitor for confidential information**
 - **Allow for file attachments/posts**
 - **Sent over SSL**
 - **Can be accidental or malicious**
 - **“Grrrr... bad day at work, my machine got a virus and I lost all my data!”**
- **Need policies to define what information is acceptable:**
 - **Should titles for IT staff be posted online?**
 - **Can you reveal when you will be on vacation?**



FI Reputation Risk

- **Employees are on these sites**
- **Identify themselves with the institution**
- **May have pictures/comments not in line with corporate policy**

“Employees should get used to a greater corporate presence in their social-networking lives, though. For companies, social networking can reveal previously unknown influence and performance in employees, and companies should tell employees that corporate conduct rules apply online, too.”*

• <http://www.zdnetasia.com/gartner-loosen-up-on-social-networks-security-62058722.htm>



Okay, So NO SOCIAL MEDIA!

- **It's not that simple**
- **What about all those customers?**
- **Great for advertising**
- **Also great for feedback!**

“The last time I had a problem with my BT broadband line at home, I mentioned it on Twitter. Within minutes BT--which is on Twitter too--was asking me about the problem. That's an example of great customer service.”

- **Need good policies and guidelines**

<http://www.zdnetasia.com/why-your-business-should-use-twitter-62056213.htm>



Protection from Technical Threats

- **User education**
 - Don't click on unsolicited messages
 - Beware of URL shortened links
 - Don't install random Apps
 - Confirm friend requests offline
- **Create a presence on well-known sites**
 - Protects against squatters / scammers
 - Advertise it so customers know it's the "real" one
 - Ensure only authorized personnel can post
- **Limit access to sites from the workplace – difficult without employee buy-in**
- **Comprehensive malware monitoring**
- **Report suspicious activity**



Things to Consider BEFORE Proceeding with SMC:

- ✓ **Strategic Plan**
- ✓ **What sites to use**
- ✓ **How will the sites be used (marketing, advertising, customer service)...**





Things to Consider BEFORE Proceeding with SMC:

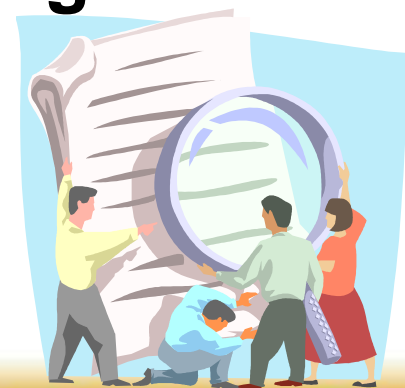
- ✓ **Who has authority over site(s)**
- ✓ **How often will it be updated?**
- ✓ **Resource allocation**
- ✓ **Employee acceptable use**
- ✓ **Record retention**





Policies/Procedures

- **No official guidance**
- **Auditors starting to ask for Social Media Policy**
- **Capitalize on FFIEC and ITRC strategies**
- **Top down approach**
- **Align business and technology strategies**
- **Set standards**





Training and Education

- **Educate customers and employees**
- **Post messages on website to never give personal or account information over public domains (facebook, twitter)**
- **Train employees on FI's policies for social media**





Are You Prepared?



twitter

