Security Issues in Social Networking

Presented by
Eric McMillen, CISSP, CISM, CISA
&
Heather Campbell, CIA

Presentation Overview

- What Is Social Networking
- Why Use Social Networking
- Social Networking Risks
- Security Best Practices

Social Networking

- Online Web services enabling people to connect with each other, share information
  - Common friends, interests, personal info, …
  - Post photos, videos, etc. for others to see
  - Communicate via email, instant message, etc.
- Major Social Networking Platforms: Facebook, Twitter, LinkedIn, Instagram

Platform Popularity

- 2.23 billion Facebook users worldwide – 2nd Qtr. 2018
  - Over 210 million in U.S.
  - Over 1.15 billion active daily users via mobile
  - Age 25 to 34, at 29.7% of users, is the most common age demographic
- Over 336 million Twitter users – 1st Qtr. 2018
- Over 562 million LinkedIn members in over 200 countries

Social Network Business Benefits

- Brand building & differentiation
- Increase customer interactivity
- Deliver better customer service
- Helps you to manage your reputation
- Increase trust in your business or brand
- Employee recruitment

What Are The Security Risks

- Brand Sabotage / Squatting
- Damage to Reputation
- Account Compromise
- Malware Distribution
- Privacy Concerns
  - Information about you that you post
  - Information about you that others post

Brand Sabotage / Squatting

- What is it? – When someone else has grabbed your bank/brand name on one of the social media sites.
- What to do.
  - Register for an account on all major social networking sites, even if it remains inactive.
  - Contact the Social Networking site and file a complaint
  - Deal with the owner of the account – last recourse.

Damage to Reputation

- What is it? – Someone, internal or external, who posts information that represents the bank in a bad light.
- What to do – External Individual
  - Monitor activity on all of your Social Network presences.
  - Google the Bank's name, as well as those of key personnel, and scrutinize results.
  - If you find a negative post or comment about your business or yourself, do not counter with another negative post. Instead, publicly offer to remedy the situation through positive action.

Damage to Reputation Cont'd

- What to do – Internal Individual
  - Establish a social networking policy, disseminating to employees, and providing periodic training
  - Restrict your business communication to the public through Facebook, Twitter, blogs, or other social media to specific individuals with appropriate media training.
  - Hiring/training staff to manage Bank's presence on Social Networking platforms (with management oversight)
  - Monitoring and reporting employee use of social media

Account Compromise

- What it is – An unauthorized 3rd party gains control over your social networking account.
- What to do.
  - Remove account access as soon as an employee with access to your social media accounts terminates
  - Ensure that you use strong passwords that are changed regularly
    - Change passwords every six to 12 months
    - Use tools like Lastpass to generate long, random-character passwords
  - Use Two-Factor Authentication (2FA) Where possible

Malware Distribution

- What it is – Techniques that can lead to downloading/installing malware, i.e. Malicious ads, Clickjacking, inbox or chat messages with malicious links from “Friends”, obfuscated URLs.
- What to do.
  - Be suspicious of friend/follow requests, ads, 3rd party applications, chat messages, etc.
  - Don’t carelessly click on lots of ads, videos, games, etc.
  - Use built-in and add-on features in web browsers to warn you of malicious sites, i.e. Anti-phishing filters in IE and Firefox, Ad Blockers, Shortened URL previews.
  - Good patching and Anti-Virus practices

Privacy Concerns

- What it is – Information that is available and can be leveraged for malicious purposes. There are three types; Information about you that *you* post, Information about you that *others* post, and Information about you the *social networking sites* collect and share with others
- What to do.
  - Be careful about what you post provide as little personal information as possible – avoid revealing birth date, address, etc.
  - Understand and customize the privacy settings in all of your social networking accounts
  - Don’t allow 3rd party applications to access your information (if possible)
  - Be careful when posting photos of employees, customers, or sensitive areas of the bank

Personal Defense Measures

- “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)

Personal Defense Measures Cont'd

- 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
  - Personal 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
  - Extreme cases:
    - Cease using social networking sites, delete accounts
    - Contact law enforcement re. relentless online harassment

Institutional Defense Measures

- Institutional defense is more complicated:
  - Monitoring employees' use of social networking sites
  - Monitoring bank's name, logo appearance on social networking sites
  - Responding to attacks on bank in a timely manner
- Encompasses all parts of an bank, not just IT dept!
- This usually entails:
  - Crafting social media policy, disseminating to employees
  - Hiring/training staff to manage bank presence on social networking sites (with management oversight)
  - Monitoring and reporting employee use of social media

Institutional Defense Measures Cont'd

- One defense approach: the HUMOR matrix

Category	Description
Human Resources	Human Resources provide companywide policies, procedures, and guidance on acceptable employee use of authorized social media tools. These guidelines and policies provide the correct processes for utilization of social media in all areas of the company, including Marketing and Information Technology.
Utilization (of Resources and Assets)	Utilization defines the capabilities of secure social media tactics and how these tactics are implemented across technologies and policies to protect a company's resources and assets.
Monetary (Considerations)	The monetary resources dedicated to creating a social media strategy and tactics as well as a security strategy have to be aligned to best serve the company.
Operations (Management)	Operations management is the day-to-day processes that must be followed to implement a security framework, from a technology perspective, as well as from an ongoing maintenance perspective. The objective is to ensure that social media is handled securely as technologies and social media platforms change.
Reputation (Management)	When all interaction scenarios with social media are calculated, the company's reputation ultimately benefits. Reputation management is the result of good or bad implementations of social media strategies as well as tactical decisions and provides a monitoring and reporting function that helps to maintain an acceptable level of security and policies over time.

Institutional Defense Measures Cont'd

- The HUMOR matrix specifies social media security outcomes, tracks bank's current status and performance goals over time
  - Outcomes can include employee training regimen, level of employee monitoring, protection of bank's IP, etc.
- Feedback loop: bank takes action to reach goals, assesses progress periodically (e.g., every 6 mo.)

Conclusion

- In my opinion, the value far outweighs the risk. I'd even say the dangers are exaggerated.
- Use social networking effectively and positively to establish new relationships, strengthen existing ones, innovate, learn, collaborate,
  and have fun.
- But beware of the risks
  so you can do your
  best to steer clear of
  them
- And **think before you click!!**

Questions?

Contact Information

Eric McMillen, CISSP CISM CISA

The McMillen Group, LLC

http://www.mcmillengroup.com

emcmillen@mcmillengroup.com

Phone: 214.810.4864

Mobile: 214.663.1563

Fax: 866.375.6006

Twitter: ericmcmillen

Heather Campbell, CIA

KCoe Isom

Senior Associate

heather.campbell@kcoe.com

Main: 316 685.0222 + 3786

Fax: 316 685.1868

Thank You!