ACUIA Webinar Education Program

Auditing Social Media in the Electronic Age

March 27, 2012

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
CliftonLarsonAllen LLP
Information Security Services

Overview

- **Social Media is here to stay…**
  - 140M Twitter users - growing at a rate of 1,382%,
  - 2008: More than 50 Banks and Credit Unions have a Facebook page

    http://www.netbanker.com
  - Today: 845M Facebook users

- **Mobile Devices:**
  - 4 Billion cell phones
  - 3 Billion w/SMS
  - 1 Billion smart phones

Types of Social Media

- Types of Social Media continue to develop…

  http://www.overdriveinteractive.com/social-media-map

Examples - Current Social Media Tools

- Blogs (e.g., WordPress, Drupal™, TypePad®)
- Microblogs (e.g., Twitter, Tumblr)
- Instant messaging (e.g., AOL Instant Messenger [AIM™], Microsoft® Windows Live Messenger, Apple Messages)
- Online communication systems (e.g., Skype™, FaceTime)
- Image and video sharing sites (e.g., Flickr®, YouTube)
- Social networking sites (e.g., Facebook, MySpace)
- Professional networking sites (e.g., LinkedIn, Plaxo)
- Online communities that may be sponsored by the company itself (Similac.com, “Open” by American Express)
- Online collaboration sites (e.g., Huddle)

High Level Pros and Cons

- Increasing brand recognition, sales
- Immediately connecting with perspective members
- Exploring new advertising channels
- Monitoring competition

v Social media sites can be used by dissatisfied customers, employees or individuals with a grudge against an enterprise to disseminate misinformation and negative information.

v Employees sharing daily activities with friends may inadvertently and unintentionally disclose information that could be damaging to the enterprise's reputation or provide information otherwise considered confidential.

Business Impact and Risk

- Social media risks resulting from unauthorized or negative postings include:
  - Disclosure of corporate assets and sensitive (privileged) information accessible to unauthorized parties
  - Violations of legal and regulatory requirements
  - Loss of competitive advantage
  - Loss of member confidence
  - Loss of reputation
  - Dissemination of false or fraudulent information
  - Inappropriate or unapproved use of company intellectual property such as logos or trademarked material

“Auditing” Social Media

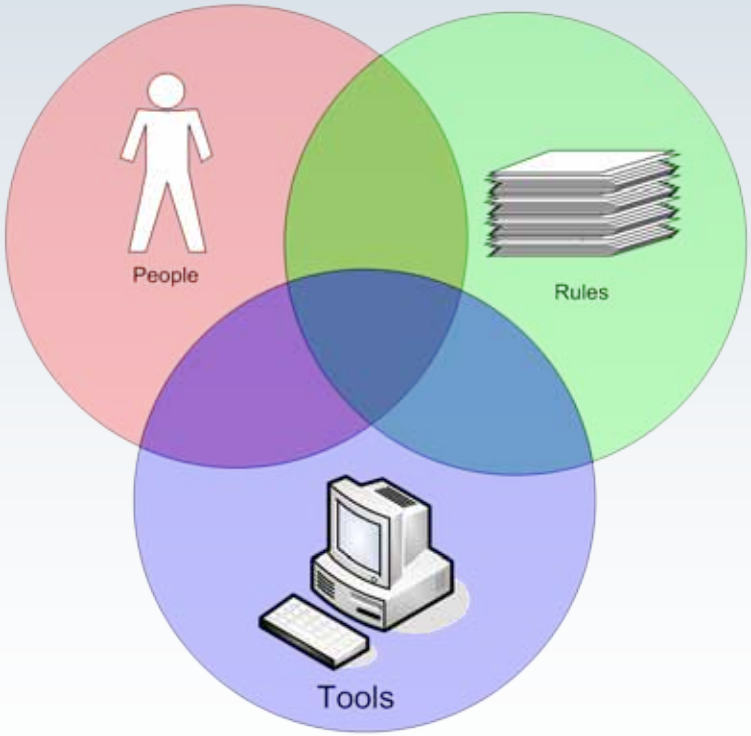
- **Different goals for auditing social media:**
  1. Audit the effectiveness of the marketing aspects
     - Ø Lots of resources on the web for this
     - Ø Not today’s focus

  2. Audit the Credit Union’s risk and security related to the communication medium
     - Ø Fewer resources on the web for this
     - Ø This will be today's focus

Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

Source: "Web Security and Commerce" by Simson Garfinkel with Gene Spafford



- Confidentiality
- Integrity
- Availability

- Everyone has a role…

Rules

- Risk Management:

Ø Risk Assessment, Risk Assessment, Risk Assessment…

  – Initial and on-going

- Policies - Documentation
  - **Acceptable use**
  - Credit Union standards
  - Personal use vs. Business use
  - Communication and expectations
  - Alignment with legal/HR and regulatory requirements
  - Contractors

  Ø Use of Social Media should be aligned with business needs

Rules

- Policies – things to consider:
  - Must respect copyrights and fair use
  - Must protect confidential information
  - Productivity matters

Rules

- Policies – things to consider:
  - Employers need to be upfront with employees:
    - Ø Employees have **no right to privacy with respect to social networking**.
    - Ø "Employers reserve the right to monitor employee use of social media **regardless of location** (i.e. at work on a company computer or on personal time with a home computer)."
  - Employees "should be made aware that company policies on anti-harassment, ethics and company loyalty **extend to all forms of communication** (including social media) both **inside and outside the workplace**."

People

- People: Communication and Understanding
  - Ø **Repetition**…
    - Acceptable use
    - Credit Union standards
    - Personal use vs. Business use
    - Communication and expectations
    - Alignment with legal/HR and regulatory requirements
    - Contractors

    - Training, training, training…

People

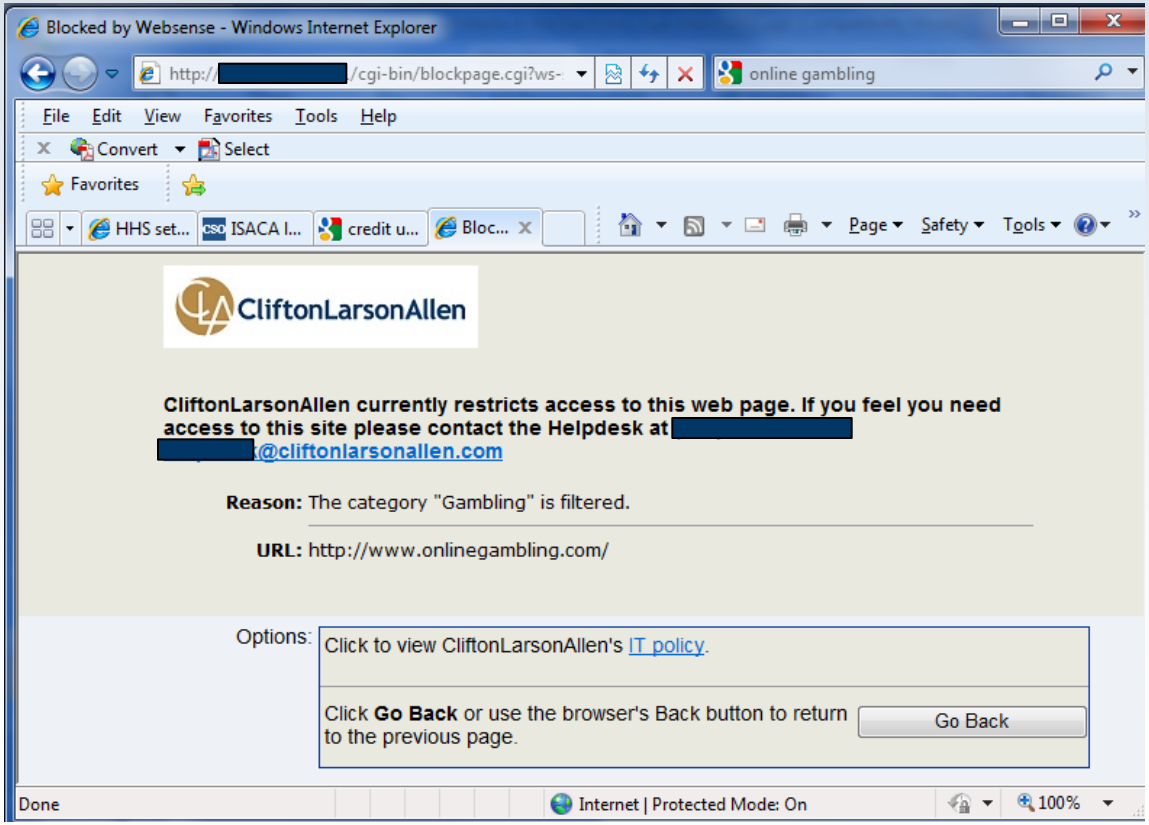
- Things to consider:
  - Be responsible for what you write
  - Consider your audience
    - ◊ Include your name, and company name where appropriate
  - Exercise good judgment
    - ◊ Refrain from comments that can be interpreted as slurs, demeaning, inflammatory, etc.
  - Understand the concept of community
    - ◊ Balance personal and professional information
    - ◊ Understand the important role that transparency plays in building a community
  - Productivity matters

Tools

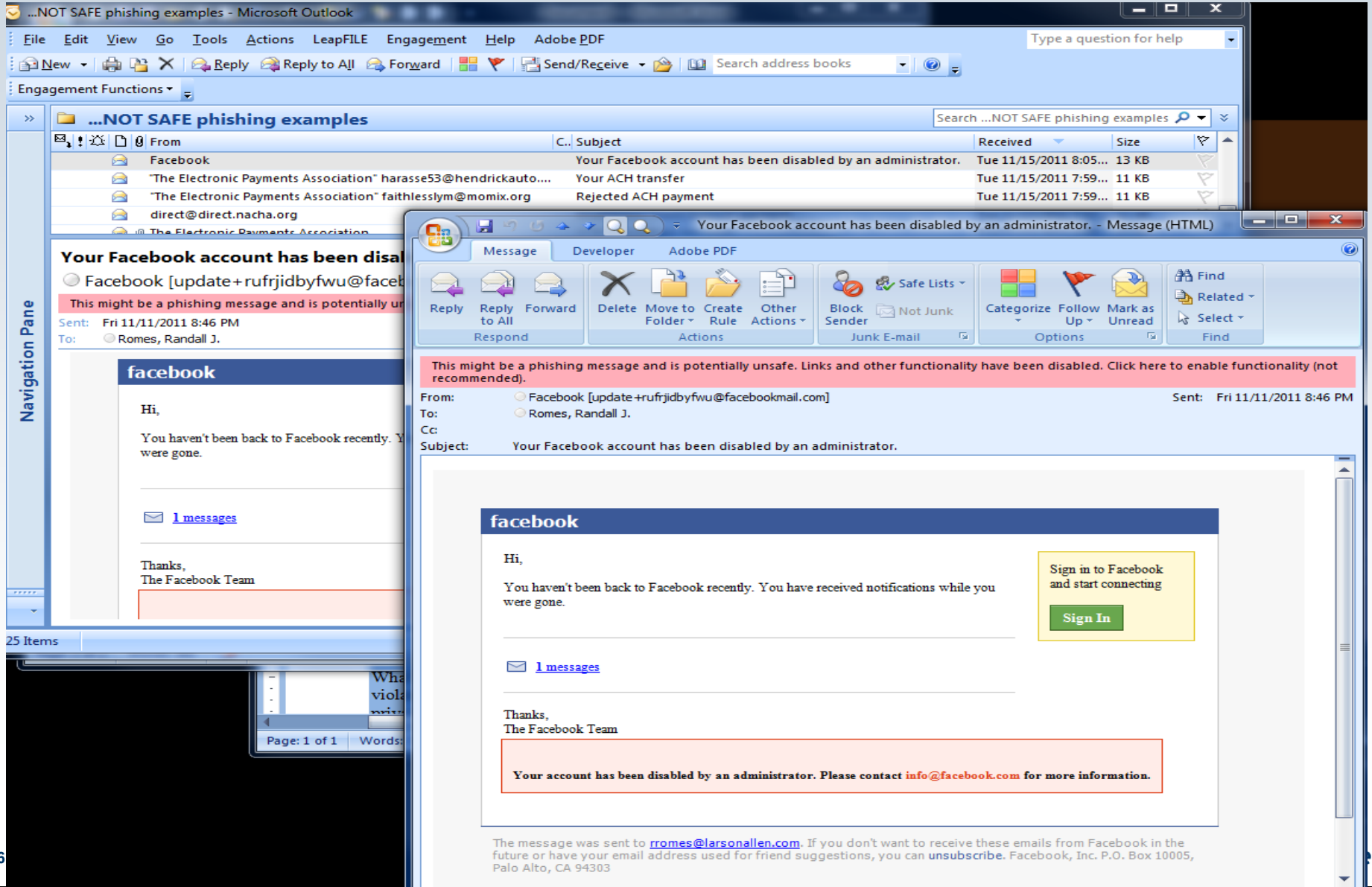
- Social Media itself can be a communication tool
  - Communicate with staff, members, and industry
  - Use social media in recruiting and applicant screening
- Monitor the sites under the Credit Union's control
- Monitor external sites

Tools

- Common infrastructure preventative controls include:
  - Antivirus and antimalware software
  - Content filtering
  - Email filtering



Tools


...NOT SAFE phishing examples - Microsoft Outlook
File Edit View Go Tools Actions LeapFILE Engagement Help Adobe PDF
Type a question for help
New Reply Reply to All Forward Send/Receive Search address books
Engagement Functions
...NOT SAFE phishing examples
Search ...NOT SAFE phishing examples
From C.. Subject Received Size
Facebook Your Facebook account has been disabled by an administrator. Tue 11/15/2011 8:05... 13 KB
"The Electronic Payments Association" harasse53@hendrickauto.... Your ACH transfer Tue 11/15/2011 7:59... 11 KB
"The Electronic Payments Association" faithlesslym@momix.org Rejected ACH payment Tue 11/15/2011 7:59... 11 KB
direct@direct.nacha.org
Navigation Pane
Your Facebook account has been disal
Facebook [update+rufrjidbyfwu@faceb
This might be a phishing message and is potentially ur
Sent: Fri 11/11/2011 8:46 PM
To: Romes, Randall J.
facebook
Hi,
You haven't been back to Facebook recently. Y
were gone.
1 messages
Thanks,
The Facebook Team
25 Items
Page: 1 of 1
Words:
Your Facebook account has been disabled by an administrator. - Message (HTML)
Message Developer Adobe PDF
Reply Reply to All Forward
Delete Move to Folder Create Rule Other Actions
Block Sender Safe Lists Not Junk
Categorize Follow Up Mark as Unread
Find Related Select
Respond Actions Junk E-mail Options Find
This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).
From: Facebook [update+rufrjidbyfwu@facebookmail.com]
Sent: Fri 11/11/2011 8:46 PM
To: Romes, Randall J.
Cc:
Subject: Your Facebook account has been disabled by an administrator.
facebook
Hi,
You haven't been back to Facebook recently. You have received notifications while you were gone.
Sign in to Facebook and start connecting
Sign In
1 messages
Thanks,
The Facebook Team
Your account has been disabled by an administrator. Please contact info@facebook.com for more information.
The message was sent to rromes@larsonallen.com. If you don't want to receive these emails from Facebook in the future or have your email address used for friend suggestions, you can unsubscribe. Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

Tools

- Monitoring controls
  - Standard infrastructure monitoring
    - ◊ Web proxies – enforce rules AND detailed activity tracking
    - ◊ Server operating system and web server log files
  - Social media alerting tools
    - ◊ Utilize the site analytics tools that come with most
    - ◊ Knowem.com
    - ◊ Social Mention
    - ◊ Trackur
    - ◊ PostRank
  - Facebook Analytics for domains
  - Google alerts and Google Analytics

Tools

- Sample Policies:

  https://www.missionfed.com/mission-federal-credit-union-social-media-public-use-policy

  http://www.ibm.com/blogs/zz/en/guidelines.html

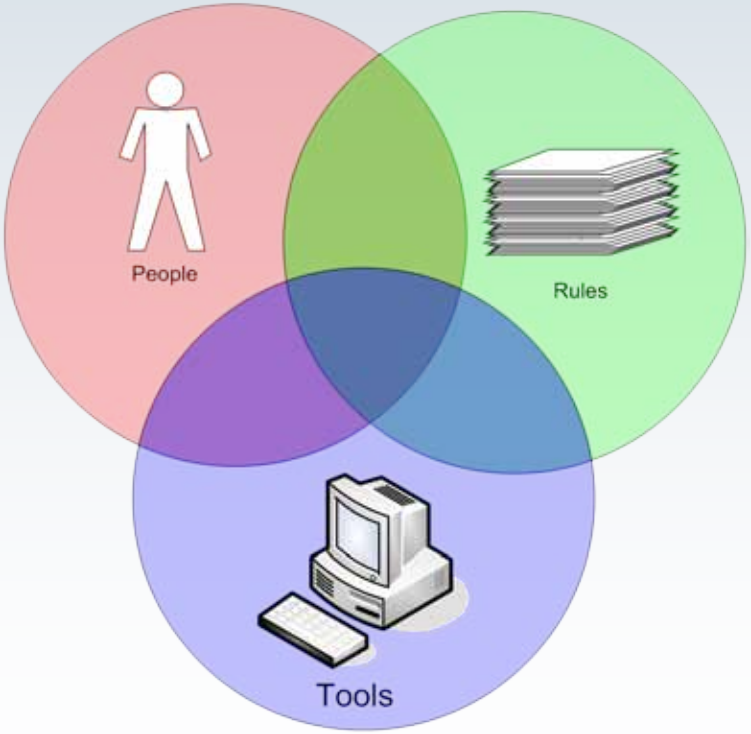
- ISACA Social Media audit program:

  http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Social-Media-Audit-Assurance-Program.aspx

Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

Source: "Web Security and Commerce" by Simson Garfinkel with Gene Spafford



- Confidentiality
- Integrity
- Availability

- Everyone has a role…

Questions?

Thank you!

Randy Romes

CliftonLarsonAllen

Information Security Services

Randy.romes@cliftonlarsonallen.com

612-397-3114