

CIPFA

4th November 2010



Simon Entwistle

techia limited

What is social networking?



Predominantly internet-based applications which allow individuals to create a profile containing personal information and interact with other users.

Are social networks relevant to me?



Public (External)

- Business Purposes
- Personal Purposes
- Public Engagement

Private (Internal)

- Business Purposes

Is there a risk to my information?



Threats

- Commercial competitors
- Criminal groups
- Disaffected employees
- Foreign intelligence
- Hackers
- Journalists
- Public
- Terrorists

Vulnerability

- Publication of content on sites
- Social interaction between users
- Technical vulnerabilities (malware, spam and phishing)

Content-related risks



- Identity theft

- Date of birth
- Home address
- Pet's name
- First school

E.g. Facebook contact sync uploads phone numbers that sync with friends pictures

Content-related risks



- Identity theft
- Photography

- Tag users
- Geo tag
- Background info
 - Car registration
 - House numbers

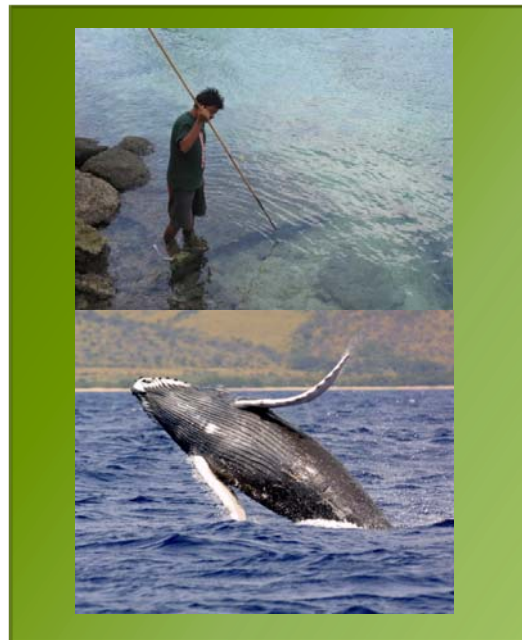
Content-related risks

- Identity theft
- Photography
- Physical security



Content-related risks

- Identity theft
- Photography
- Physical security
- Social engineering



Content-related risks



- Identity theft
 - Photography
 - Physical security
 - Social engineering
 - Reputational damage and corporate liability
- Employees can post information that is
 - Deliberately wrong
 - A personal opinion taken to be the official line
 - Mistaken
 - Information must comply with legislation, e.g. Data Protection Act, Freedom of Information Act.

Content-related risks



- Identity theft
- Photography
- Physical security
- Social engineering
- Reputational damage and corporate liability
- Release of sensitive information

- Sensitive
- Protectively Marked
- Information can aggregate

Content-related risks



- Identity theft
- Photography
- Physical security
- Social engineering
- Reputational damage and corporate liability
- Release of sensitive information
- Cyberbullying, cyberstalking, cyberharassment

- A forum for bullying and harassment

E.g. false profiles to publish defamatory or embarrassing comments

Content-related risks



- Hijacked accounts

- Most passwords are weak and guessable

- Used as a vector for further attack

- E.g. thousands of twitter users continue to have their accounts compromised including a french diplomat last week, President Obama, firstdirect, Ed Miliband.

Content-related risks



- Hijacked accounts
- Profile Squatting

▪ A profile set up without the individual or organisation's permission

▪ E.g. David Miliband

Content-related risks



- Hijacked accounts
- Profile Squatting
- Inappropriate or offensive content
- Employers have a duty of care to protect their staff from this type of material

Content-related risks



- Hijacked accounts
- Profile Squatting
- Inappropriate or offensive content
- **Disclosure of information**

- Website development faults
- **Third party applications**

E.g. Facebook banned developers this week for collecting contact information and selling this on to advertising firms

Content-related risks



- Hijacked accounts
- Profile Squatting
- Inappropriate or offensive content
- Disclosure of information
- Terms and conditions

- Social network terms and conditions vary
- Some own all content
- Some sell this content to third parties

E.g. LinkedIn sell information, Facebook own content.

Content-related risks



- Hijacked accounts
 - Profile Squatting
 - Inappropriate or offensive content
 - Disclosure of information
 - Terms and conditions
 - Time-wasting and bandwidth
- Employees use social networks excessively
 - Videos can be bandwidth-intensive

Social interaction risks



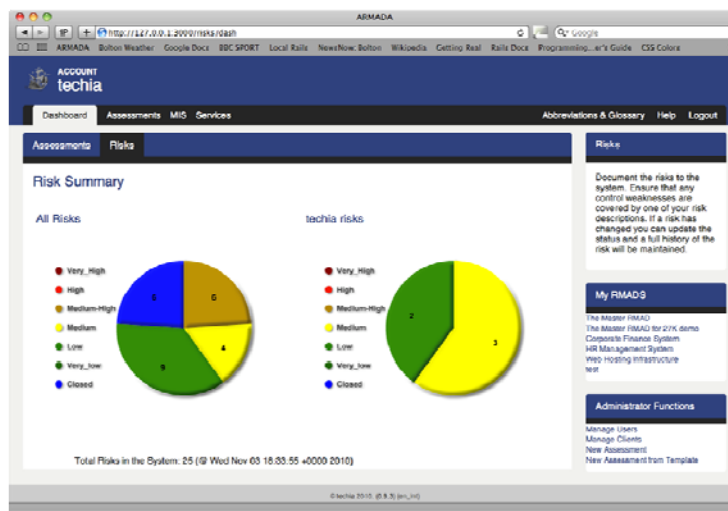
- Lack of discrimination regarding contacts
- Lack of control over postings by other users

Malware, Phishing and Spam



- Phishing
 - Spam
 - Socially distributed malware
 - Malware from third parties
 - Application vulnerabilities
- Attacks can appear to come from friends
 - Short URLs prevent knowledge of the target and frequently link to malware

E.g. Koobface



Perform a risk assessment



Assessment Action Plan

- Review the risks (reduce/accept/avoid/...)
- Define policy
- Select controls
- Educate the user
- Control access internally
- Control external pages
- Most risks are dependant on user behaviour

THE USER IS THE MAIN THREAT

References and Further Reading



- CPNI Good Practice Guides
- www.getsafeonline.org
- A Strong Britain in an Age of Uncertainty: The National Security Strategy



Simon Entwistle

CLAS, CISSP, CISM, ITPC

techia limited

www.techia.info

simon@techia.info

07595 674316