

Social Security

Secure Computing, Privacy & Etiquette
with Social Media

James Teiser

jteiser@atomystic.com

January 21, 2010

dp&a

Business Reputation

- “There is no such thing as bad publicity except your own obituary.”
 - Brendan Behan
Irish author and dramatist (1923-1964)
- **With respect to your business and the nature of social media, this is patently untrue.**

dp&a

Don't...

- Operate computers without protection.
- Let anyone and everyone represent your business.
- Reveal company secrets or confidential info.
- Be vulgar or mean-spirited in online public forums.
- Be dragged into the mud in online public forums.
- Spam with e-mail or social media communications.
- Divulge customer info.
- Be fraudulently opportunistic or too slick.
- Be stupid.

dp&a

Secure Computing Basics

- Apply a firewall to your network.
- Run a commercial grade anti-virus/anti-malware program on all computers.
- Regularly run software updates on all computers.
- Stop the cycle of spam.
- Don't be phished.
- Be careful about where you click (i.e. beware of URL shorteners).
- Encrypt e-mail.
- Take time to properly set up privacy preferences.

dp&a

Write a Security Policy

- Create an approved application list.
- Define appropriate web use at work.
- Require strong passwords.
- Enforce consequences.
- Educate and inform your employees.
- Educate and inform your customers.

dp&a

Who, What & Where...

- Decide who can speak on behalf of your business.
- Spread it around: assign specific topics/areas of expertise to specific people.
- Define what's confidential and "fair game," and communicate this to everyone at your company.
- Decide which social media sites are most important, and assign accordingly.
- Train employees about proper behavior and etiquette in online public forums.

dp&a

Social Media Etiquette

- Bloggers/Twitterers/etc. should identify themselves as employed/paid by your company.
- Protect customer info and egos.
 - BCC: (not cc:)
 - Remind customers not to share personal info.
- Be opportunistic, but don't try to be too slick.
 - Twitter #hashtags (<http://news.bbc.co.uk/2/hi/uk/8116869.stm>)
 - Artificially large networks
- Don't be a social media spammer.

Data Mining & Social Networks

- People share...
 - dates of birth
 - e-mail addresses
 - home addresses and telephone numbers
 - family and relationship info
 - professional info
 - educational info
 - affiliations
 - contact lists
 - pictures and videos
 - clues to passwords and challenge questions

dp&a

Advertising, Spam & Fraud

- “Legitimate” but unwanted advertising
 - Think about all those quizzes and 3rd-party apps on Facebook
- Data miners/list brokers
 - ➡ Spam spam spam spammy spam
- Viruses, trojans, worms and other malware
 - Koobface (<http://news.cnet.com/koobface-virus-hits-facebook/>)
 - URL shorteners (e.g. [Bit.ly](#), [TinyURL](#))
- Phishing and spear-phishing
- Identity theft

Do...

- Regularly communicate your **safe and ethical security and privacy policies** to your employees, contractors, partners and customers.
- Leverage social media to its maximum potential to promote your business.
- Be smart and use common sense.
- **Protect your business' reputation and goodwill with customers and the general public.**

dp&a

Facebook Privacy Settings

- <http://www.facebook.com/privacy/explanation.php?ref=pf>
 - <http://www.facebook.com/policy.php>
 - <http://www.facebook.com/settings/?tab=privacy&ref=mb>
 - <http://www.facebook.com/editapps.php?ref=mb>
 - <http://www.facebook.com/editaccount.php?ads>

dp&a

Thank You

Be Smart & Be Safe

James Teiser

e-mail: jteiser@atomystic.com

Skype: [jamesteiser](https://www.skype.com/people/jamesteiser)

Twitter: [gonzo2dot0](https://twitter.com/gonzo2dot0)

GoogleVoice: 415.704.1849

dp&a