Cybersecurity and Social Media

SecurIT360
The physics of securing IT

Social Media today includes a wide variety of mediums and technologies in which users can generate their own content or comments and broadcast it publicly via internet websites. It is accessible by computers and mobile devices, and in many cases, postings or comments can be made anonymously.

- Facebook
- Twitter
- Myspace
- LinkedIn
- Blogs
- Message Boards
- Business Networking
- Business Reviews
- Dating Sites
- Gaming Sites
- Photo /Video Sharing Sites
- Comment Sections on News Sites

Social media represents opportunity and risk to every company.

Consider the following statistics.

- More than 70% of online adults and 92% of under-30's use social media sites.
- Facebook has more than 1 Billion users!
- More than 200 Billion tweets go out each year.

Social Media can impact a business in many ways, both positive and negative. The uses and impacts of social media can be complex and far-reaching. When used effectively, it can be a great marketing tool for promoting a company's image and the products and services they sell. Unfortunately, it can also be one of the fastest ways to impact a business in a negative manner. It can be used to organize protests and public relations attacks against a company when a person or group of people dislike something or someone associated with that company.

The corporate perspective of social media can be very complex. We will mostly focus on personal use of social media in this article, but these are a few good guidelines to consider in corporate use of social media.

- Carefully consider if your company will use it in an official capacity.
- If so, be sure to set policies for use that will reflect the proper messaging from a marketing, image, and public relations perspective.
- Whether is used in an official capacity or not, you should have HR policies in place to set expectations for employee's social media use that could impact the company.

My social media is my business. What does that have to do with my company?

While many people consider social media to be a personal thing, our personal use of it can have a tremendous impact on our employers. Our positive or negative use of social media may be linked to our employer or other associations. We see examples every day in which a company is praised or condemned, based on the social media actions of an employee. It is also a good thing to consider for anything we do. Recognition of positive or negative behavior is often broadcast via social media.

dburns@securit360.com

Cybersecurity and Social Media

SecurIT360
The physics of securing IT

Like other Cybersecurity issues, there are human behavior and technical considerations to address.

- Keep personal and business social media sites very separate. Social media cannot be erased.
- Slow Down! Especially if you are angry or highly emotional.
    - Take a few extra seconds to re-read your posts on social media, just as you do with e-mail, to reduce embarrassing errors.
    - A seemingly simple tweet or Facebook posting about business can have profound consequences for us and for whoever tweeted or posted it.
- Know how to set the privacy settings on every social media site before using it.
- Learn how to recognize social engineering, such as requests to watch videos, click links or go to websites.
- Social media has become a breeding ground for cybercriminals, scams, fraud and identity theft.
- Be wary of e-mails that claim to come from any of your social networks.
    - Many of them are hoaxes and could be malicious.
- Assume security will fail, and everyone, including your boss, could see your personal updates and photos.
- While much of the impact is based around image and messaging, there are significant cybersecurity aspects as well.

From a technical perspective, it is important to understand that your social media accounts can be hacked like any other account. The key thing about a social media hack is that it can be used to publicly ruin your reputation.

- If your social media account has been hacked or compromised, take these steps immediately.
    - Change your password and make it very strong.
    - Reset all sharing and make it the most restrictive you can.
    - Notify anyone who may have received rogue messages that your account was comprised.
    - Temporarily revoke access to all apps and add-ons associated with the compromised account.
    - At home: Scan your computer with up-to-date, reputable antivirus software.
    - At work: Contact IT Security Immediately.

As always, develop a “cyber-defense” mindset to protect yourself AND your company.

If you would like to learn more about Cybersecurity and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250