Social Network Security

With the popularity of social networks skyrocketing, many people—including employers—are beginning to worry about security. Though these websites started off as personal networking tools, they are quickly becoming commonplace for businesses, too.

Precautions for Social Media Use

Remember that protecting the reputation and credibility of your employees is just as important as protecting your business reputation, especially since business and personal relationships and connections continue to mesh via social networks. While these tips do not take the place of an effective social networking policy, they are a good starting point for companies new to social media.

Password Protect

As a general rule, never enter your password into third-party sites unless they are trusted sites.

You should have, or will need to create a strong password that:

- Is at least eight characters long
- Does not contain user name, first name, surname or company name
- Does not contain a complete word
- Contains a combination of uppercase letters, lowercase letters, numbers, spaces and symbols

Use Lists and Privacy Settings

Many of the social networking sites today allow tiers of access to personal or business profiles for offering limited access to certain user groups. Stress the importance of these tools to employees, making sure those that connect with clients or co-workers may only view appropriate content.

Also, consider using these functions for your company's account. These controls can help you keep tabs on your competition without allowing them to see everything you post, or they can prevent those with malicious intentions from finding out your location or names of employees.

> Protecting your business reputation is important—especially now as business and personal connections continue to mesh on social networks.

Filter Carefully

On most social networking sites, the user has control over his or her own posts but not over what others decide to share. Think carefully about the image you are trying to portray and whether other users' postings help or hurt that image. That is not to say you should remove every constructive criticism or negative comment, but you should remove spam and any content that is inappropriate or vulgar.

Talk to your employees about the impact others' postings may have on their image and how it could jeopardise their job.

Most importantly, be sure your company's social network password(s) are not the same, or similar, to any other passwords used in the past. Phishers, those who obtain username and password combinations and use them maliciously, will try to open other accounts

The content of this Risk Insights is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

and gain access to money or proprietary information. Stress these tips with employees too, as a comprised or misused employee account may impact your business negatively as well.