WHO'S PEEKING OVER YOUR SHOULDER?
FOUR STEPS TO SECURING YOUR SOCIAL MEDIA

Adventist Risk Management, Inc. | Weekly Newsletter
Who’s Peeking Over Your Shoulder?

Four Steps to Securing Your Social Media

Imagine sitting in a public setting working on your computer. Suddenly, you get the odd feeling that someone is peeking over your shoulder, reading every detail that you type. Without the use of proper security when using social media, your information is vulnerable to being breached. Even in the privacy of your own home, someone in cyberspace might be checking out your private data, with plans to use it illegally.

Continue reading...
Copyright © 2015 Adventist Risk Management, Inc, All rights reserved.
You are receiving this email because you opted in at our website or someone signed up on your behalf. If you did not sign up for this list or wish to discontinue receiving correspondence from Adventist Risk Management, Inc., please click on the 'UNSUBSCRIBE' link.

Our mailing address is:
Adventist Risk Management, Inc
12501 Old Columbia Pike
Silver Spring, MD 20904

Add us to your address book
unsubscribe from this list update subscription preferences
Imagine sitting in a public setting working on your computer. Suddenly, you get the odd feeling that someone is peeking over your shoulder, reading every detail that you type. Without the use of proper security when using social media, your information is vulnerable to being breached. Even in the privacy of your own home, someone in cyberspace might be checking out your private data, with plans to use it illegally.

Social media provides many benefits, such as keeping in touch with friends and connecting those with similar interests, but communicating in cyberspace comes with a measure of risk. According to the National Crime Prevention Council, the main dangers of social media are over-sharing information, sharing information with the wrong people, posting the wrong photos, and services which track users' location. Sharing too much information online is dangerous because personal information in the hands of others can lead to identity theft.

With new social media networks forging connections and current networks constantly updating, how does one stay social media savvy and keep their organization and/or family safe?

**Step 1: Know Your Social Media**

Knowing the six basic types of social media helps you understand their use and audience.

1. **Social Networks** like Facebook and LinkedIn connect people with similar interests or backgrounds.
2. **Bookmarking Sites** such as Delicious and StumbleUpon allow users to save and share links to other websites and resources.
3. **Social News** sites including Digg and Reddit allow users to post news items or links to outside articles with the option to vote on the best items.
4. **Media Sharing** sites such as YouTube and Flickr are platforms for uploading and sharing a variety of media including pictures and videos.
5. **Microblogging** sites like Twitter focus on short posts updated regularly and sent to a group of subscribers.
6. **Blogs and Forums** such as Tumblr and Wordpress allow users to share a variety of content and hold conversations through commenting on that content.

**Step 2: Secure Your Social Media**

A. **Know and use the privacy settings for all types of social media.**
   - Take a survey of what social media you subscribe to and read over the privacy policy.
   - Find out who owns the content and who can see it once it is posted.
   - Privacy policies and settings are updated periodically and when networks change owners. When updates are required, take a moment to check and refresh your settings.

B. **Create a secure password and a unique username for each online account**
   - A password should be eight or more characters long, include uppercase and lowercase letters, and at least
one number and one special character.

- A unique username should not include any personal information, such as your name or email address.
- A solid password and unique username adds another level of security to your information, and makes it harder for others to access your account.

C. Once your account is secure, always log out of social media when you are done. Leaving yourself logged in is making your account accessible to anyone who accesses that device.

Step 3: Protect Personal Information

Protect your information by being careful what and how you post. Even if your account is set to private, it could still be hacked and the information could go public.

In order to protect your personal information, don’t give it away. Hide as much information as possible and don’t fill out optional information. Knowing the state and city you were born in can be used to acquire your social security number and other identifying information that can be used to steal your identity.

Information that should never be shared on social networks include: social security numbers, birth dates, home addresses, phone numbers, and all PIN, bank account, and credit card numbers.

Step 4: Post Wisely

Post and use social media wisely to create a positive online image and keep yourself safe. Posted information can share where you are and what you are doing. For example, some social networks allow users to “check in” at their current location, and posting vacation photos while on vacation shares your present location with cyberspace. These features share that you are not at home and your house is ripe for robbing.

Content posted online creates an online identity that impacts your life. Follow your employer’s social media policy and consider your current online footprint. Are you sharing information that other people shouldn’t know? Could it hurt someone else? Is this representing the person you want to be?

Protecting your information online is as important as keeping it secure in real life. These four steps can help you use social media safely.

by: ANNA BARTLETT
WRITER & EDUCATION SPECIALIST

Adventist Risk Management, Inc.