Like

Rampart Group LLC

Investigation & Security Services

Tip *of the* Week

Social Media Security Threats

Social networking has dramatically changed the way we interact with others. Applications like Facebook and Instagram make it easy to catch up with far-flung friends and update family members on our latest adventures, but social media can create major risk to our personal security.

Hackers and identity thieves prowl social media networks looking for victims. When using social media sites, it is important to know the privacy risks involved and what precautions to take to protect our personal information.

Here are 5 tips to keep your personal information out of the wrong hands:

1. Create strong passwords- The more complex your password is, the harder it is to guess. Steer clear of using names, birthdates, or social security numbers. Also, consider using a password that combines letters, numbers and symbols and don't use the same password for multiple sites. If a hacker guesses one, they've guessed them all.

2. Remember the "about me" is optional- Most social media sites offer the opportunity to fill in a great deal of information about yourself, but that doesn't mean you have to. Many identity thieves hack victims email accounts by simply using the personal information available on your social media profile. Avoid making your birthdate, phone number and address publicly available information.

3. Install strong antivirus and anti-spyware software- Hackers can use spyware and fraudulent links to interject malicious code onto your computer to steal your information, hold your devices hostage for ransom and steal banking information. Avoid clicking on links you're unsure of. Shortened URL's like bit.ly and owl.ly links used on Twitter are particularly susceptible to hackers. Try a link scanner like URLVoid or Sucuri to determine if a link is safe.

4. Master privacy settings- All social media sites offer various privacy settings to limit post viewing to specific audiences. Take the time to explore these options. Both Facebook and Twitter allow you to create lists of people who can see specific posts but remember, just because an image is indexed as private on Facebook, it could still show up on a Google image search. *If you don't want it public, don't post it!*

5. Keep the updates to a minimum- When you alert your friends that you're heading on a five-day cruise to Mexico, you're also letting potential thieves know your home or business will be unoccupied. When you go on a vacation, don't post specifics, and consider waiting until you return to post pictures online. Be aware that tagging family members in pictures could give away password guessing information like mother's maiden name or children's names and birthdates.

Remember that when you post something online, that information is no longer private and can easily fall into the wrong hands without proper security measures. Take a few necessary steps and avoid becoming a victim of identity theft and fraud.

Kathy Leodler
Chief Executive Officer
PI License #3555
kathy.l@rampartgroup.net
(360) 981-2703

Paul Leodler
Executive Vice President
PI License #4180
paul.l@rampartgroup.net
(360) 981-3397

Rampart Group offers security consulting services to help you put best practice solutions in place to protect your most valuable assets - People, Property, Products, Information, and Business Reputation.

Follow Us:

Missed and Article or Tip? Click here to visit our Archives!

Archive

Email: info@rampartgroup.net | Website: www.rampartgroup.net | Tel: (800) 421-0614