CONSUMER ADVISORY

October 2013 By Attorney General Tom Miller

Social Media Safety & Security

There's a lot to like about Facebook, Twitter, Instagram, LinkedIn, YouTube, and the many other social networking sites that allow you to post your pictures and videos, thoughts and information about you—and see what others post. But what you post or who you network with can also leave you vulnerable to long-term embarrassment, identity theft, criminals, and unwelcome strangers.

Your Profile

Be very careful about what you include in a personal profile. Do you really want to post your address and your phone number? Are there other details, like something as simple as posting your pet's name or your mother's maiden name, that a criminal could use to answer a "security question" to access your financial accounts?

Posting and Protecting Personal Information

When you post personal information, including pictures, treat it like it's there for anyone to see—even if you think it's private or restricted. Assume that any family member, current or future employer, school administrator, and stranger can see it and post the same information or photo on their site. Also assume that removing something doesn't necessarily make it go away—it may be impossible. Think twice about posting when you're traveling away from home, or routinely "checking in" to places that a potential stalker could track. And think twice about meeting face-to-face with a person you know only through online contact. "Untag" photos that others post of you, if you feel a photo of you is inappropriate. Be sure you understand a social network's privacy policies and privacy settings.

"Friending"

Are you "friending," connecting, or providing personal information to someone you've never met in person? Are you sure that person is really who they claim they are? Do you really want people you have never met to see your profile and posts?

Unusual Request from a "Friend?"

If someone you *think* you know sends you a request through social media that involves money or clicking on an unusual link, it may be from an account that someone has hacked or spoofed (a hacker appearing as your friend). These requests could be "emergency" pleas for money, offers to share a sudden windfall of money, unusual job or investment "opportunities," or clicking on a link associated with a posting that seems out of place. If you have even a small doubt about the authenticity of an email, check it out before responding.

Careful Clicking, Viruses & Spyware

Be careful when you click on links and downloading attachments, even if they appear to come from someone you know. Both can expose your computer to viruses or spyware. Be cautious about downloading attachments. Use your firewall, anti-virus and anti-spyware software, as well as spam filters, and be sure to keep your software and browser up to date.

Strong Passwords

Use strong passwords and don't send them to anyone. Use unique passwords, and don't use a simple word that you'll find in the dictionary. If you use the same password for several accounts, those accounts are particularly vulnerable. When you're on a public computer, don't allow the computer to store your login information.