Are You Practicing Safe Social Networking?

CYBER SECURITY AUGUST 2017

Who Else Is Online?

Social media sites are not well-monitored playgrounds with protectors watching over you to ensure your safety. When you use social media, do you think about who might be using it besides your friends and connections? Following are some of the other users you may encounter.

- Identity Thieves.
  Cybercriminals need only a few pieces of information to gain access to your financial resources. Phone numbers, addresses, names, and other personal information can be harvested easily from social networking sites and used for identity theft. Cybercrime attacks have moved to social media, because that's where cybercriminals get their greatest return on investment.

- Online Predators
  Are your friends interested in seeing your class schedule online? Well, sex offenders or other criminals could be as well. Knowing your schedule and your whereabouts can make it very easy for someone to victimize you, whether it's breaking in while you're gone or attacking you while you're out.

- Employers.
  Most employers investigate applicants and current employees through social networking sites and/or search engines. What you post online could put you in a negative light to prospective or current employers, especially if your profile picture features you doing something questionable or "less than clever." Think before you post a compromising picture or inflammatory status. (And stay out of online political and religious discussions!)

How Do I Protect My Information?

Although there are no guaranteed ways to keep your online information secure, following are some tips to help keep your private information private.

- Don't post personal or private information online!.
  The easiest way to keep your information private is to NOT post it. Don't post your full birthdate, address, or phone numbers online. Don't hesitate to ask friends to remove embarrassing or sensitive information about you from their posts, either. You can NEVER assume the information you post online is private.

- Use privacy settings.
  Most social networking sites provide settings that let you restrict public access to your profile, such as allowing only your friends to view it. (Of course, this works only if you allow people you actually know to see your postings — if you have 10,000 "friends," your privacy won't be very well protected.)

Are You Practicing Safe Social Networking?

CYBER SECURITY AUGUST 2017

- Review privacy settings regularly.
  It's important to review your privacy settings for each social networking site; they change over time, and you may find that you've unknowingly exposed information you intended to keep private.

- Be wary of others..
  Many social networking sites do not have a rigorous process to verify the identity of their users. Always be cautious when dealing with unfamiliar people online. Also, you might receive a friend request from someone masquerading as a friend. Here's a cool hint — if you use Google Chrome, right-click on the photo in a LinkedIn profile and choose Google image search. If you find that there are multiple accounts using the same image, all but one is probably spurious.

- Search for yourself.
  Do you know what information is readily available about you online? Find out what other people can easily access by doing a search. Also, set up an automatic search alert to notify you when your name appears online. (You may want to set alerts for your nicknames, phone numbers, and addresses as well; you may very well be surprised at what you find.)

- Understand the role of hashtags.
  Hashtags (#) are a popular way to provide clever commentary or to tag specific pictures. Many people restrict access to their Instagram accounts so that only their friends can see their pictures. However, when someone applies a hashtag to a picture that is otherwise private, anyone who searches for that hashtag can see it.

My Information Won't Be Available Forever, Will It?

Well, maybe not forever, but it will remain online for a lot longer than you think.

- "What happens on the web, stays on the web."
  Information on the Internet is public and available for anyone to see, and security is never perfect. With browser caching and server backups, there is a good chance that what you post will circulate on the web for years to come. So: be safe and think twice about anything you post online.

- Share only the information you are comfortable sharing.
  Don't supply information that's not required. Remember: You have to play a role in protecting your information and staying safe online. No one will do it for you.