Smart Tips for Safe Social Networking

Many of us do a great deal of socializing online as we catch up with old friends and make new ones using sites such as Facebook, Twitter, LinkedIn, and YouTube (to name a few).

While social networking sites are a convenient way for us to keep in touch, these sites are also an easy way for criminals to gather our personal information, which is then used to steal our identities, our money, or even our personal property (for those of you who post your vacation plans on these sites – a big fail BTW). To make your social networking experience a safe one, we have listed a few tips to help you "out-smart" the cyber crooks and other evil doers:

1. Tighten your social networking account's privacy settings. Limit access to who can see your personal profile. Directions on how to do this varies by site with most sites providing FAQs or other modes of help for securing your account. Be aware that these actions will not guarantee your privacy, since many sites such as Facebook have experienced security breaches in the past.

2. Don't divulge too much information. Never post detailed information about:
   - Where you live or work
   - Your children
   - Your birth date
   - The state where you were born (could be used to guess the first 3 digits of your SSN)
   - Your telephone number
   - Vacation plans/activities
   - Any information about your boss or coworkers that could get you in hot water.

3. Be careful whom you accept as friends.

4. Be very careful using public Wifi. It is very easy for criminals to get access to your computer, mobile device and personal information via unsecure wireless networking.

5. Be cautious of third-party applications that gather your personal information or infect your computer with malware.

6. Use strong passwords and different passwords for each account.

7. Use malware protection software.

8. Keep all of your software updated with the latest security patches.