SOCIAL NETWORKS: Be Careful What You Share

A lot of people use social media sites – such as Facebook, LinkedIn, Twitter, Google+ and Instagram – to stay in touch with family and friends, meet new people and interact with businesses. However, identity thieves can use social media networks in hopes of learning enough information about individuals to be able to figure out passwords, access financial accounts or commit identity theft.

Identity thieves create fake profiles on social networks pretending to be financial institutions and other businesses, and then lure unsuspecting visitors into providing Social Security numbers, bank account numbers and other valuable personal information. They also create fraudulent profiles and send elaborate communications to persuade "friends" to send money or divulge personal information.

Here are some safety measures you can take to protect yourself on social media.

- **Check your security settings on social network sites.** Make sure they block out people you don't want seeing your page. If you have doubts about your security settings, avoid including information such as your birthday or the year you graduated college. Otherwise, though, experts say it is OK to provide that kind of information on your social media pages.
- **Take precautions when communicating with businesses.** If you communicate with a company on social media, keep in mind your posts could become public, even though you can protect your posts to some extent through your account settings. You should never include any personal, confidential or account information in your posts.

  Before posting information such as photos and comments, you should research the page's privacy policies to find out what can be shared with other parties, including companies who want to send you marketing emails and how they will keep personal information secure.
- **Be cautious about giving third-party programs or apps (such as sites for games or quizzes) the ability to use information from your social networking pages.** These third parties may use information from your page to help you connect with others or build your network. They could also be selling your information to marketing sites and others, possibly even to people who might use your information to commit fraud.
- **Periodically search to see if someone has created a fake account using your name or personal information on social networking sites.** Checking common search engines for your name and key words or phrases (such as your address and job title) may turn up evidence that someone is using your information in a dishonest way.

Heritage BANK

Information provided by the FDIC