Bank of Tennessee
Carter County Bank
Mountain Community Bank
CARTER COUNTY BANK AND MOUNTAIN COMMUNITY BANK ARE DIVISIONS OF BANK OF TENNESSEE MEMBER FDIC

Social Media and ID Theft

How ID Thieves use social media to get your information

Using social media usage is now standard practice most Americans' daily lives. According to a 2014 Nielsen Ratings Report, internet users continue to spend more time with social media sites than any other type of site with almost half (47%) of smartphone owners visiting social networks every day.

Because you must divulge some level of personal information in order to use and fully benefit from social networking sites, the risk of identity theft is greater for people who use them. Below are some of the ways that you might put yourself at risk of identity theft:

- Using low privacy or no privacy settings
- Accepting connections from unfamiliar people
- Downloading free apps and games for use on your profile
- Participating in quizzes which may require you to divulge a lot of personal information
- Clicking on links that lead you to other websites, even if the link was sent to you by a friend or posted on your friend's profile
- Not fully logging out of the social media site from a computer that the general public can use
- Falling for email scams (phishing) that ask you to update your social networking profiles
- Using no or out-of-date security software to prevent malicious software from being loaded onto your computer and stealing personal information

Here are a couple examples of how identity theft can happen through a social networking site:

Example 1: You receive a message from a social network connection which has a link to a funny video. You click on the link but the video doesn't show. Your social network friend's profile has been hacked, and now a form of malicious software has been downloaded onto your computer because you clicked on the link. This software is designed to open a way for an identity thief to take personal information from your computer. Then the program automatically sends a similar email or post to everyone that you are connected with, asking them to "view the video."

Example 2: Cyber criminals can create a page that looks just like the home page of a social networking site. These criminals will send you an email that looks like it is from the social network with a link to fraudulent site and ask you to enter your username and password. Once they have your credentials, they can access all the personal information you have posted on the social media site and in your account profile.

How to better protect yourself:

- Enter the least amount of information necessary to register for the social media site.
- Create a strong password and change it often. Use a mix of upper and lower case letters, numbers, and characters that aren't easily guessable such as birthdates, addresses, last names, etc.
- Use the highest level privacy settings that the site allows. Do not accept the default settings.
- Be wise about what you post. Do not announce when you will be leaving town. Other things you should never post publicly: your address, phone number, driver's license number, social security number (SSN) or student ID number.
- Only connect to people you already know and trust.
- Read privacy and security policies closely. Some major social networking sites will use or sell information about you in order to display advertising they believe might be useful to you.
- Verify emails and links in emails you supposedly get from your social networking site. These are often designed to gain access to your user name, password, and ultimately your personal information.
- Install a firewall, reputable anti-spam and anti-virus software to protect your information-- and keep it up to date!
- Be certain of both the source and content of each file you download. Don't download an executable program just to "check it out." If it's malicious software, the first time you run it, you're system is already infected. In other words, you need to be sure that you trust not only the person or file server that gave you the file, but also the contents of the file itself.
- Beware of hidden file extensions. Windows by default hides the last name extension of a file, so that an innocuous-looking picture file, such as "susie.jpg," might really be "susie.jpg.exe," an executable Trojan or other malicious software. To avoid being tricked, unhide those pesky extensions, so you can see them.
- Use common sense. When in doubt… don't open it, download it, add it, or give information you may have doubts about sharing.