SOCIAL

NETWORKING SAFETY

ETSU Police 423-439-4480
Or 911
www.etsu.edu/dsp
bucprevention@etsu.edu

The following 10 tips offer guidelines in managing the information that gets out there about you via social networking and can help keep you safe:

No Such Thing as Private The internet is like an elephant -- it never forgets. While spoken words leave little trace and are quickly forgotten, written words endure in the online environment. Whatever you post, tweet, update, share -- even if it's deleted immediately afterwards -- has the potential to be captured by someone, somewhere, without your knowledge. This is especially true of social networking sites including private messages shared between two people and postings to a private group. There is no such thing as "private" in the world of social media because anything you put up can potentially be grabbed, copied, saved on someone else's computer and mirrored on other sites -- not to mention hacked by thieves or subpoenaed by law enforcement agencies.

A Little Bird Told Me Every time you use Twitter, the government keeps a copy of your tweets. Sounds crazy, but it's true. According to the Library of Congress blog: "Every public tweet, ever, since Twitter's inception in March 2006, will be archived digitally at the Library of Congress.... Twitter processes more than 50 million tweets every day, with the total numbering in the billions." And experts predict the information will be searched and used in ways we can't even imagine.

X Marks the Spot Be cautious about using geo-location services, apps, Foursquare, or any method which shares where you're at. When it was first introduced, Facebook's "Places" This can turn your home into a public place. This apps can be used for cyberstalking as well.

Separate Work and Family Keep your family safe, especially if you have a high profile position or work in a field that may expose you to high-risk individuals. Some women have more than one social networking account: one for their professional/public lives and one that's restricted to personal concerns and only involves family and close friends. If this applies to you, make it clear to family/friends to post only to your personal account, not your professional page; and don't let the names of spouses, children, relatives, parents, siblings appear there to protect their privacy. Don't let yourself be tagged in events, activities or photos that may reveal personal details about your life. If they show up, delete them first and explain later to the tagger; better safe than sorry.

How Old Are You Now? If you must share your birthday, never put down the year in which you were born. Using the month and day are acceptable, but adding the year provides an opportunity for identity theft.

It's Your Fault If It's Default Keep track of your privacy settings and check frequently update and change settings, and often the defaults tend to make public more information than you may be willing to share. If an upcoming update is advertised in advance, be proactive and investigate it before it launches; it may offer a window during which you can privately edit or remove content privacy settings enable you to review content in which you've been tagged by friends before they appear publicly on your page. This should include posts, notes, and photos. It may seem tedious, but it's much easier to deal with a

small amount each day than to have to go back through weeks, months and even years to ensure that any and all content related to you puts forth an image you're comfortable living with.

It's A Family Affair Make it clear to family members that the best way of communicating with you is through private messaging or email -- not posting on your page. Often, relatives who are new to social media don't understand the difference between public and private conversations and how they take place online. Don't hesitate to delete something that is too personal for fear of hurting Grandma's feelings -- just make sure you message her privately to explain your actions, or better yet, call her on the phone.

You Play, You Pay...in Loss of Privacy Online games, quizzes, and other entertainment apps are fun, but they often pull information from your page and post it without your knowledge. Make sure that you know the guidelines of any app, game or service and do not allow it unfettered access to your information. Likewise, be cautious about responding to notes shared by friends along the lines of "10 Things You Didn't Know About Me." When you answer these and post them, you're revealing personal details about yourself that may enable others to figure out your address, your workplace, the name of your pet or your mother's maiden name (often used as an online security question), or even your password. Do enough of these over time and someone who is determined to learn all about you can read the answers, cross-reference information obtained through your friends' pages, and glean a surprising amount from these seemingly casual revelations.

How Do I Know You? Never accept a friend request from someone you don't know. This may seem like a no-brainer, but even when someone appears as a mutual friend of a friend or several friends think twice about accepting unless you can concretely identify who they are and how they're connected to you. In many professional circles involving large organizations, all an "outsider" has to do is obtain one friend on the inside and it snowballs from there, with others thinking that a total stranger with no personal connection is an unfamiliar co-worker or occasional business associate.