9 TIPS to be cyberSAFER

1 When you work on both Home and Work computers:
DO NOT exchange documents between the two computers. The home computer's security may be less than the work computer. Whether via email, CD or flash drive, the risk of damage to the work system is too great. Keep work data on a work computer and home photos and documents on the home computer.

2 When you use multiple family computers at home:
AVOID using a less-secure computer (like a child's) for sensitive data, like on-line banking or storing family photos. Cyber criminals can steal money, identity or images of a family member.

3 When you hit the SAVE button:
BE AWARE that information lives forever on the internet and is identified by search engines. So, think twice before you post; because bad guys look at this stuff.

4 When you post a photo from your cell phone camera:
AVOID posting with GPS Coordinates. Check your phone settings to make sure this functionality is off. An attacker can track your location without you being aware that the coordinates are automatically sent. Also, when posting photos on vacation, be aware that you're announcing that you're not at home to potential threats.

5 When you browse the Internet at a Public Hot Spot:
DO NOT divulge sensitive details. However, if you do something like online banking, make sure it is encrypted – Look for the lock icon. If you are on a public computer, such as at a library or hotel, DO NOT go to your bank account.

STOP your devices from automatically connecting to available public Wi-Fi.

MAKE SURE the hot spot is a legitimate Hot Spot by asking someone who works at the location for the Wi Fi connection details before connecting.

6 When you post life details to Social Network sites:
USE the privacy controls for each social network. This requires some research as they are different for each.

AVOID posting data that could be used to target you. Keep your information private – such as your address and vacation schedules. Also, photos with location data embedded in the file could be used for harm.

7 When you access sites where you are an ACCOUNT Holder:
LOOK for the "Padlock" in the address bar area – a green padlock is best. This icon says a site is secure. However, it is difficult to see this on a phone.

8 When you send E-mail:
FOLLOW BEST PRACTICES for e-mail privacy such as using different usernames for home and work e-mails, and different passwords for every account. Also, be wary of any e-mail requesting personal information.

9 When you set up any account:
USE very complicated passwords that are unique, strong, and hard to discover. Write these down and keep them in a safe area. Use different passwords for each site.

DISABLE the "Remember Password" function on your computer by going to "Tools", then "Internet Options", then "Content", then "Auto Complete Settings", make sure that "User names and passwords on forms" are not checked

USE TWO FACTOR AUTHENTICATION to make it harder for potential cyber criminals to gain access and steal personal data. Simply use a username and password together with a piece of information that only you know. When providing answers to a questions – such as "Your Mother's Maiden Name"– make up a pretend answer to further ensure your online safety.