Tip of the Month September, 2012

Back to School Safety Message

The long summer break is over and as students head back to school they have good reason to spend academic time online. Paperwork is becoming a thing of the past because students now prefer to track assignments, grades and events using their school's online system, which is available in most cases now-a-days, especially if the student is college bound!

Students share and transmit a lot of personal information online. They not only use academic online tools that require personal information details, but young people generally are incredibly active social network users. This is true whether the student is a ninth grader or a college senior. Parents are not exempted either!

Fran Maier is the president and executive chair of TRUSTE, the leading online privacy solutions provider. She shares the following ten tips with students:

1. Password-Protect Your Computer/Smartphone/Tablet

You store a lot of personal data (like photos) on these devices, which may also save automatic logins to your email and social networking accounts. Someone could easily abuse this information if you leave your device unattended — an important consideration outside of the classroom as well. A solid password contains a mix of letters, numbers and symbols and does not contain common words. In other words, rethink your "1234" iPhone passcode.

2. Consider Theft-Recovery Applications

These applications can geo-locate your lost device and/or allow you to remotely login. Electronics theft on college and high school campuses is a real problem. Installing such an application on your computer, smartphone or tablet could mean the difference between recovering your device and losing it forever.

3. Review Your Social Networking Privacy Settings

This tip is especially important for high school seniors who've submitted college applications, and for new grads applying for their first jobs. Avoid accepting "friend" requests from people you don't know.

4. Protect Your Online Reputation

Social networks may not be the only component of your online identity. Blogs, personal websites, discussion forums and photo accounts also reflect online activity. With little effort, people can piece together your various online accounts and activity — even accounts under fake names that you thought were anonymous. With every piece of content that you share, ask yourself: Would I want my parents, teachers and future employers to discover this? Once you post something on the Internet, it can very difficult, if not impossible, to remove it.

5. If You're a Minor, Lock Down Your Location

Many social networks and mobile applications allow you to tag your current geographic location. For your physical safety as a minor, the visibility of your location should only be available to your closest friends — if at all. Parents should talk to their kids about online predators and ensure they're not sharing their location with strangers.

6. Do Your Back-to-School Shopping Securely

Some of the best back-to-school shopping deals can be found online, but not all shopping websites are created equal. At minimum, you'll disclose your name, home address, phone number and credit card information to complete a purchase, so make sure that each website is secure. Look for privacy and reputation seals on the website. The URL of checkout WebPages that require your personal information should begin with "HTTPS," indicating that the website encrypts your personal information during transmission.

7. Avoid Online Gossip

While school-age gossip and bullying seem unavoidable, remember that the effects can be magnified online, be it through email, chat or social networks. Inappropriate photos of or comments about someone else can go viral in a matter of minutes — within a few hours your entire school could potentially see what you've written or shared. Viral gossip is almost always permanent, and can only come back to haunt you.

8. Don't Share Passwords With Friends

It might be tempting to share your passwords with friends, but it's better to keep them to yourself. For instance, your password to a gaming account might be

similar or identical to your password for another, more sensitive account, like email. Moreover, sharing your passwords may put other friends or family members at risk, especially if your accounts include their personal information.

9. Beware of Identity Theft

College students especially are targets for identity theft. Beware of the signs: If you receive notices about accounts you didn't open, or if you see unexplained charges on your credit card statements, be suspicious and follow up.

10. Get a Lock For Your Locker/Desk/Closet

This tip is as old as school itself, but it's especially important in our digital age. Chances are your locker or desk doesn't just hold your books, jacket and lunch – it may also store your smartphone, computer or tablet devices which are typically loaded with personal information. If you're in a high-traffic dorm room, consider investing in a laptop padlock that secures the device to your desk.

Stay safe and study hard!

For more information on this and any other data protection concern you may have, please email us at dataprotection@bahamas.gov.bs or visit our website www.bahamas.gov.bs/dataprotection.

Remember "Privacy is the Best Policy"