Cyber Security Awareness

SLC CYBER Security: Travel safely with your devices

As you prepare for the break in the semester and to head home or to other wonderful destinations, we understand that there are a lot of things on your mind. We want to help you plan ahead so that device and information theft are the least of your worries. While you are traveling, here are some of the tips and tricks that we want to pass on. And On behalf of the IT Service Department, we hope you have a Happy Holiday!

Here at SLC we want to keep you safe so check out our 8 ways to stay safe while traveling.

CYBER Security: Travelling

8 Ways to Stay Safe While Travelling

1. **Password protect device:** feels like every month this is mentioned, but changing your password before or and after your trip is advised. This prevents anyone who may have seen your password from being able to access your account. To reference what makes a strong password look back at our September blog for some guidelines.
2. **Turn off location tracking (GPS tracking, App specific tracking as well)** apps like Facebook and Twitter can tell people where we are, but this also tells strangers where you are or where you aren't! When posting about going away for any amount of time, make sure you can see the post, or don't post about it until you have returned. Posting about trips in social media is just like hanging a sign on the door saying "No one is home, come on in!"

3. **Backup your data before you leave:** image writing your final paper for the toughest course of school. Only just as you are about to finish, your computer crashes. But instead, this is your entire computer, everthing you have ever saved, and

instead of a crash, somehow your computer gets lost while you're away! Can you imagine trying to recover everything? Backing up your data before you leave is not only a smart thing to do to free up some space, but it might even let you relax! The school does offer unlimited storage on OneDrive by Microsoft as an option before you take off this Holiday season.

4. **Beware of public Wi-Fi hot spots:** hot spots have been a life-saver to us all, but they also come with a lot of risk! Public Wi-Fi hotspots open your device up to a wide range of situations from easier access for viruses, to devices being watched by other uses on the network. If there is a secure network, use it. Avoid online banking on public Wi-Fi, and if you using a cell phone, use applications instead of the website for sites like Facebook and Twitter.

5. **Turn off Wi-Fi and Bluetooth when not using:** when you're not using Wi-Fi or Bluetooth, turn them off. Not only will this save you some battery life, but it will also cut down on the ability to be tracked online. Wi-Fi and Bluetooth are also looking for a connection. These connections create a 'road map' of sorts that can be used to locate you.
6. **Turn on "find my phone" and enable feature to wipe data:** This feature is now built in to almost all cellphones being made and allows you to find your phone, if the worst case possible should happen! Unfortunately, there are two downfalls, location services must be on, and you must have battery life. But having had to use this, it was remarkable how accurate the mapping can be.
7. **Don't connect your cellphone to unknown devices (use wall charger instead of a public computer). In reverse, don't connect anything to your computer that you do not know!** Connecting your device to an unknown computer, or your computer to an unknown device is just asking for issues! Whether you are travelling or not you should always be aware of what you are connecting to due to the risk of Malware, viruses, Trojans, you name it. Even if your device doesn't become infected, you may transfer the infection to another device. Yes, cell phones can get viruses. Apple devices are not immune either!

8. **Update your device, software and anti-virus:** another way to keep your devices safe is by keeping them up-to-date. Keeping software, anti-virus software and operating software up to date will help to limit the threats that you may experience. Often your software programs will tell you when it needs to be updated, but some programs may need to be updated more often.

A good idea is to look for updates once a month for programs you use often. For your anti-virus make sure to update it a night or two before you leave!

Additionally, if travelling to a dangerous location, you may consider installing an app to track your location. This will allow you to set-up a safe contact, in case you need to hit a panic button your location information is sent to them, advertising your last known location, for emergency services.

There are now apps being created that will use location services to track your location and will send this information to a selected contact when you hit a 'panic button'. These apps are great when you are travelling to locations that may not be as safe as we would like. There are a number of these apps and some offer additional services and may be tailored to user demographics. If you are travelling, please remember your personal safety is of the utmost importance!

Now that you're an expert in travel safety for electronic devices… SHOUT OUT TO US! Let us know your top Travel tips by tweeting us or mentioning us on FB!

For more topics on e-security click here!

Got a great idea for next month's SLC CYBER Security – timely information, you need to know? Share it! Let us know here or tweet us using #SLCE-security