



Cyber Security Awareness

SLC CYBER Security: timely information, you need to know ...

Each year the College has handfuls of USB flash drives handed in to the Lost and Found located in the IT Service Desk. Each year, these little devices get more and more dangerous! This isn't to say you shouldn't use them, just be careful about when and where you use them! USB Flash drives, as we know them, have been around since the early 2000's and not much has changed from the outside, but on the inside... WOW! These little things can pack a punch. They now come in memory sizes that would have been unimaginable. Portable hard drives have also grown in capacity in leaps and bounds as well. The fact that we can now get a 4 terabyte portable hard drive is just crazy, given that just a few years ago it was a luxury to have a portable hard drive.



CYBER Security: Electronic Device Safety

1. **Don't mix and match.** If you are using USB flash drives for school and personal information, don't use the same one for both! This opens your personal information up to unnecessary exposure. If you are using a portable hard drive, look at ways to segregate your information. If the device comes with encryption or password protection, become familiar with using it for all of your files.
2. **Finders, Keepers? Not so fast...** We know how tempting it is to plug in the flash drive you find on the ground, but please, for your computer safety, DON'T! At the college USB Flash drives, and anything electronic, should be turned in to the IT Service Desk. This is to protect your computer and the school systems from Malware.
3. **Safety features have a purpose, please use them.** A large number of USB Flash Drives and portables now come with a range of security features included when you purchase them. These range from password protection to encryption. Sometimes you have to pay more for these features, but they are well worth the expense when it is your safety on the line. If you don't want to spend the money on the features, you can always password protect the individual files. Hundreds of videos and websites can walk you through how to do this based on the type of file you are working with!



4. **For those tech savvy people: Disable Auto run.** When you plug in any USB connected device, the computer automatically tries to run certain protocols. By disabling these, you have more control over what happens and when. This may seem complicated for some beginners, but if you are comfortable with technology, this may just save you from a very nasty Malware attack.

5. **We hate to keep repeating ourselves, but have you updated your antivirus this month?** Antivirus protection seems like an obvious item, especially since we have mentioned it multiple times! We still see people come in to our office with no protection on their computer and wonder when we tell them it sounds like a virus... Please don't be one of those people! There are many different programs to choose from ranging from expensive to free, and that you download only one and from a reputable source.



CYBER Security: Safe Alternative

At the College, we like to give you a safe alternative! So, all students have access to OneDrive. This is accessible through your student email, so no more lost Flash Drives or forgotten ones. The OneDrive account is accessible anywhere that you have internet service, even on many mobile devices. Another bonus to the OneDrive, its unlimited space! Use as much or as little as you need!

Now that you are an expert in device security... **SHOUT OUT TO US!** Let us know your top five electronic device 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**.