



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Incorporating cyber security in the classroom

Cyber security is quickly becoming a much-needed skill in the world regardless how basic. Technology has become part of our lives be it schools through online learning, homes through smart appliances or transport system through self-driving cars. Online learning for students has positive impact in that students have more learning alternatives; they can learn in a comfortable environment and parents are more involved in their children's learning.

Despite such positive impact of learning online, there are a number of risks students and teachers could face during an online class such as classroom hijacking and security breach of student data. This could cause harm to an individual and institution depending on the type of attack or risk and platform being used. For example, breach of student data could expose the identity of the students and lead to identity theft and intrusion of privacy. This can damage the mental health of a child who is still growing up.

How then can we incorporate cyber security in the classroom?

There are different and creative ways we can do this while conducting an online class. Children learn and understand better by observing, listening, exploring, experimenting and asking questions. Teachers should ensure that they make cyber security learning highly interactive and include visuals. This could be through videos, activities and exercises.

- Use of separate login accounts

During online learning, students should not use a shared account to login into a computer while learning. This is because having shared accounts have more risks involved. For example, out of curiosity a student could accidentally share private information from the shared computer or account belonging to their parent or guardian like birth certificate, driver's license number, bank account number, passport number and email address without knowing the effects it may cause.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

- Disable or cover Webcam when not in use

Hackers have come up with more sophisticated ways of spying an individual through use of web cameras. When there is a class that does not require use of web camera students should disable or block them using web camera cover.



- Use of passwords and password managers

Password enables one to protect information in our devices and give access to only those with an authorized password to gain access.

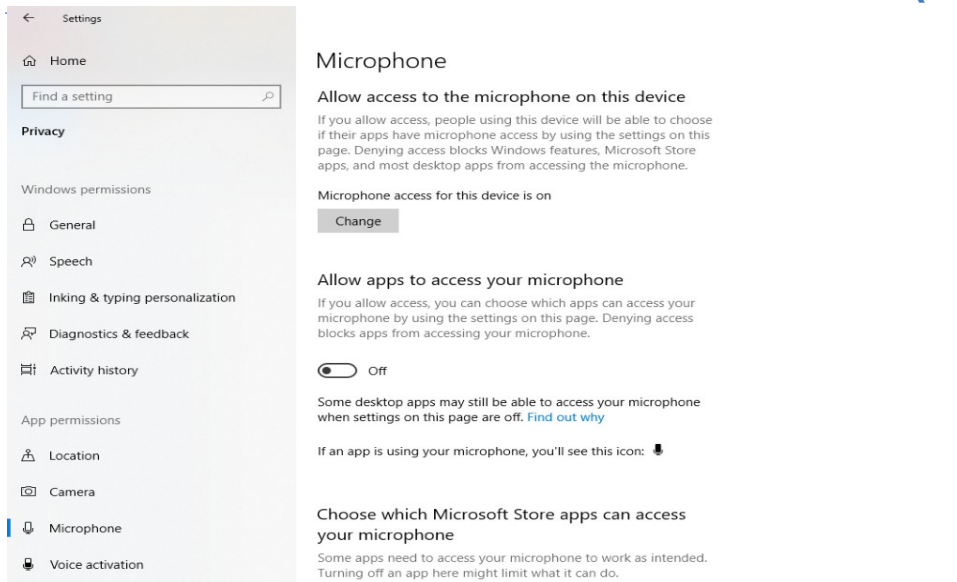
Students can use password managers instead of writing down their passwords in books or papers that could be easily accessible by anyone. Password managers will enable one to generate secure passwords that cannot be reused instead of using names and date of birth. Password managers enable students to access legitimate saved links like school portal and prevent clicking on rogue links that may resemble the school portal.

- Disable microphones

Another way a hacker can spy is through microphones to eavesdrop on conversations. Students should disable their microphones when not in use to avoid hackers from listening in a private discussion.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)



- Use of student friendly search engine

Students should use kid friendly search engines such as kiddie, kidrex and wackysafe. These are safe search engines that allow students to search for information, images, videos, and news that's appropriate for them.



[image from kiddie.co]

- Identifying Personally Identifiable Information

Before starting a class, teachers can bring up with the conversation of what Personally Identifiable Information (PII), why it is important not to share this



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

information and the risks of sharing this information. The students could participate by identifying what they think PII is and examples.

- Updating computer software

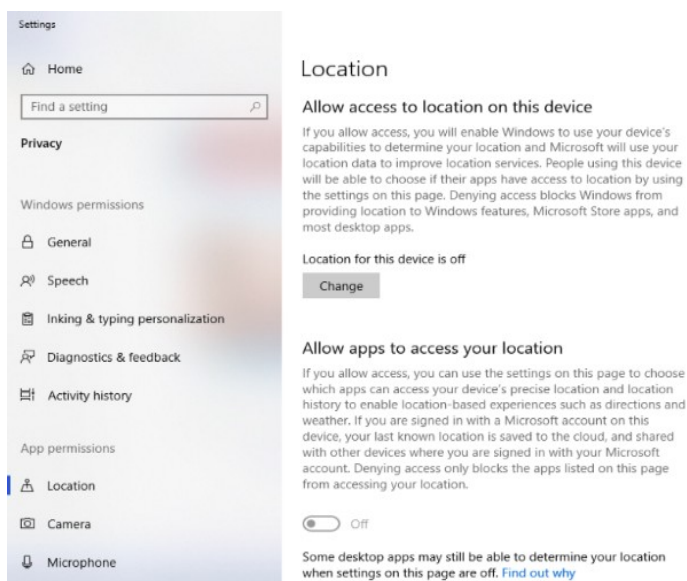
Students should ensure that their devices are up to date. They should constantly check for any available software updates and consult with their parents, guardians or teachers before doing so. Updates will enable your device to have current software and decrease the likelihood of cyber-attacks.

- Shut down or lock devices

Students should shut down or lock computers, laptops or tablets when not in use. These Devices should be protected using strong passwords. Devices left on when not in use are at risk of attacks and access by unauthorized persons.

- Turn off location services

Devices have a feature that can attach data such as web search and pictures to the location. In order to have anonymity, disable such features so that your movements cannot be tracked based on your online activity.



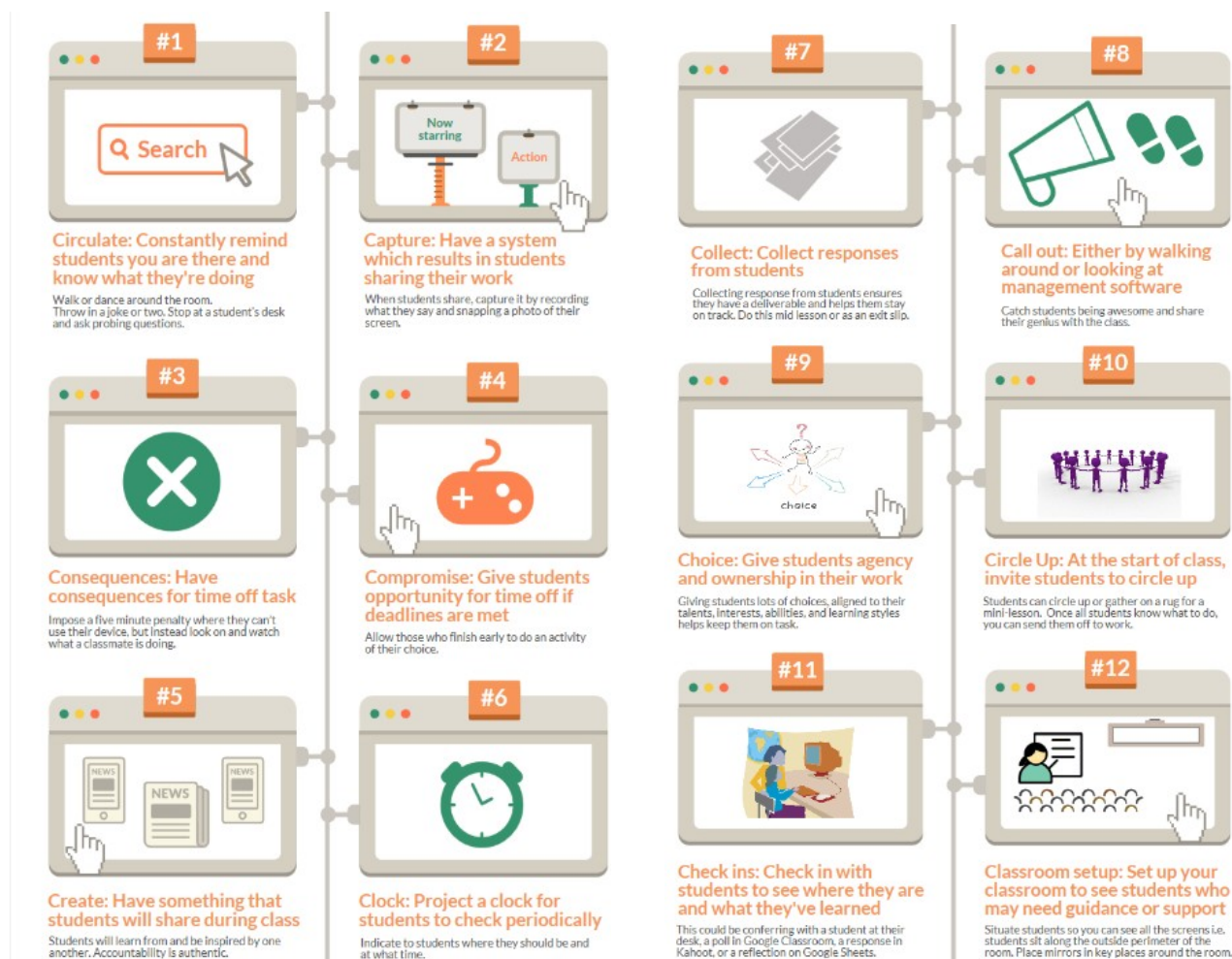


CYBERSECURITY TRAINING FOR TEACHERS (CTT)

- Links and Downloads

Clicking on links and downloading content from the internet, especially if malicious, could cause harm such as stealing information like passwords, slowing down or crashing a device, etc. Students should consult with their parents, teachers and guardians before clicking on links they are not sure of or downloading content from the internet, especially, on emails.

Technology is the future of online learning. However, most educators can have a difficult time adjusting to this. Teachers can use the following guide to aid them in managing an online class.

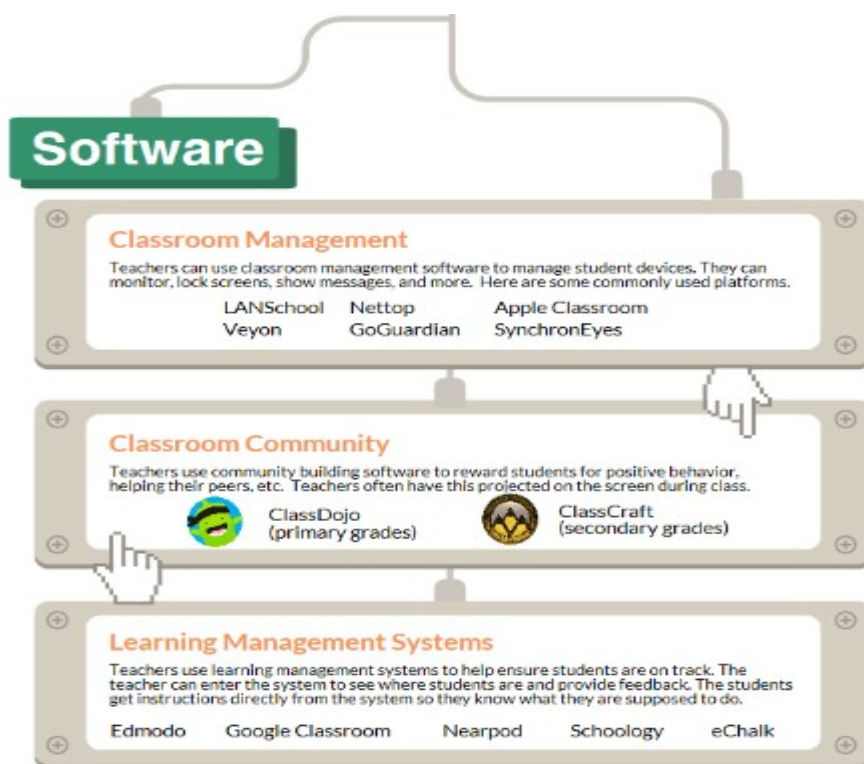


[images from: elearninginfographics.com]



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

The teachers can have a software application to assist them manage student devices by monitoring, locking. The application can be used to view progress and provide feedback.



[image from:

elearninginfographics.com]

International Telecommunication Union (ITU), a specialized agency of the United Nations is responsible for issues that concern information and communication technologies. It has an [activity book](#) for students and a [guide for teachers](#) to facilitate teaching on online safety.