



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Week 1 Online Learning Platforms Transcript

Having looked at the CIA triad, we're now going to explore various online learning platforms and their security concerns. Online Learning is the future of learning. With rapid advancement of technology, learning has never been easier, both teachers and learners can access quality education via online platforms. Learning has greatly evolved over the years, the traditional class involved face to face instructional learning. Teachers and educators then incorporated technology to aid face to face learning.

For example, through the use of projectors and computers. Today, we have blended learning which is a mixture of face to face and online learning. For online learning, students can access materials remotely. Some courses are usually offered fully online without any face to face interaction with the instructor. This is known as distance learning. Learning institutions have resorted to distance learning due to the corona pandemic to actively engage their students. Online Learning is usually supported by various platforms. These platforms include, Learning Management Systems, Student Management Systems and Video Conferencing Platforms.

A Learning Management System or LMS is a software application used for administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs or learning and development programs.

LMSs are designed to support teachers and teacher educators in administering and managing accessible courses. Learners can also pace themselves and access the course material from virtually anywhere. The learner's experience can be personalized therefore aiding in better user experience. Learning Management Systems usually store very confidential data such as training content, student's information and teacher information. This information is very crucial in the administering of online courses. Therefore, it should be protected to prevent any data breaches.

Some of the commonly used LMSs include, talent LMS, Canvas, Moodle, and mooKIT. However, LMSs usually have some security concerns that we should all take into consideration. Most LMSs are vulnerable to malware.

Malware is any malicious software that can be used to divulge any confidential information or to gain unauthorized access into a system. Malware can also be used to obtain confidential information such as passwords and usernames. Once an attacker obtains the username and the password, they can easily login to your account and change the password, therefore, you will not be able to log in as a legitimate user.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

LMSs are also vulnerable to password guessing attacks. In these attacks, the attacker usually tries different combinations of password and username and tries to guess the correct one. If a user is using a weak password, it is easily guessed and therefore, an attacker can easily gain access into your account. Having explored these two security concerns, it is important to know what security features are available to you for you to implement and prevent these cyberattacks. This learning management system should also be updated regularly. This is because vendors continually release updates that address various security concerns that were found in previous versions.

We also need to use very strong password for our LMS accounts. This is because strong passwords are not easily guessed, and therefore, the attackers will not be able to gain access into your account.

Another platform that supports online learning is Student Management Systems or SMSs. These are platforms that are used to manage student data in any learning institution. Student data is very critical and sensitive in any learning institution. Therefore, it should be protected effectively and properly. A leak of this data could damage a school's reputation and brand image. Some of the key functionalities of SMSs include, Student Information Storage, faculty management, report generation, access portals for students and parents, as well as enrollment or registration management.

Some of the popular SMS is in the market include open SIS and school time. Just as we've mentioned for LMSs, student management systems also vulnerable to malware. This is because SMSs store very critical and sensitive data that is very alluring to attackers, attackers will therefore use malicious software to try and gain access into the Student's Management Systems.

Attackers are always trying to get you to click on links and download malware. For example, they will send you spam emails with various links attached. And when you click on these links, you download malware into your computers or even into your mobile phones. It is very important to consider the security features that are available in the Students Management System. This will prevent attackers from gaining any unauthorized access.

Additionally, remember to use very strong passwords to login into the Student Management System. You should also avoid sharing passwords or even writing them down. This is because unauthorized personnel such as students can get a hold of these passwords and use them to login



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

in to the Student Management System. Students having these passwords can even use the system to modify their grades.

Lastly, we have video conferencing platforms. These platforms are used to hold live sessions and webinars. These live sessions usually simulate a real classroom and therefore, students and teachers can interact and promote engagement during remote learning. For example, during these live sessions, students can ask real time questions and teachers can provide guidance. Some of the popular video conferencing platforms include Zoom, Microsoft Teams, and Google Meets.

With video conferencing platforms an intruder joining the call is a major security concern. Without proper implementation of security features, unauthorized people can access confidential training sessions and disrupt the sessions. The links to these sessions are usually obtained from social media platforms as well as unsecured networks such as public WiFi. Once intruders have joined the session, they usually post inappropriate content as well as share links that leads to malicious websites on the chat feature or the video conferencing platform. This makes the video conferencing platform vulnerable to malware. We'll also look at various case studies of such incidents where intruders have interrupted a class or training session.

Privacy is also another consideration when using video conferencing platforms. Most platforms usually offer a recording feature where teachers are able to record training sessions and share with their students for future reference. It is important for teachers and teacher educators to seek permission from the parents before sharing such content. When sharing the recorded sessions, it is also important to share them over secure channels. Before using any video conferencing platform, make sure to explore all the security and privacy features that are provided by the platform.

Once you've explored those, make sure that you've implemented them before any virtual meeting.

Having looked at the various security concerns, let us now look at the various guidelines that are provided for teachers and students when using video conferencing platforms. When conducting online classes, teachers should engage their students on video conferencing do's and don'ts. These include, you should ask your students to mute their mics, they can enable the microphone where they need to talk to the rest of the class.

You should also advise students to join using their real names. This will enable the teacher to properly identify and verify the students. Ask the students to only share information related to



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

their lesson on the chats. You should also let them know of the consequences of breaking any of the classroom rules. Students should also use the latest version of the video conferencing solution such as Zoom or Microsoft Teams.

Some of the guidelines for teachers include: be careful about the documents you show on the screen. This will avoid accidental sharing of confidential data. Make sure to verify the student's identity to prevent intruders from joining. This can be done by enabling the waiting room. In this you should also advise your students to use their real names for easier verification. You should also not allow the students to rename themselves for easier class management. You should also not allow students to share their screen unless it is needed for class presentations.

If need be, remove any students or parents who do not follow the classroom rules this will maintain order. The teacher should also disable private messages to foster transparency and easier management of the chat feature. Lastly, you should always reiterate the guidelines at the beginning of each class. This will engrain security into your students and ensure they exercise caution while online.

We will now explore various considerations when selecting technology to support online learning.

Before selecting any technology to use for online learning, you should ask and answer some of these questions. Is the online learning technology accessible? How easy is it to use the technology? And is the online planning technology safe and secure for school use? What are some of the security features that are provided by the online learning technology?

By asking these questions, you'll always make sure that security is a consideration during the selection process. As we have seen, security is an important consideration in online learning. As a teacher, you should ensure that all the systems and applications you use for online learning are secure. This will protect you and your students from cyberattacks, and protect your information.

This brings us to the end of this topic. In this topic, we learnt about various online learning platforms. This includes the Learning Management Systems, Student Management Systems, and Video Conferencing Platforms. We also looked at the security concerns and what to do to make sure that these platforms are secured. Next, we're going to have a discussion on these online learning platforms.