CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Online Learning Platforms Write-up

Objectives

- Familiarize with platforms that support online learning such as LMS and SMS
- Explore various security risks.

Introduction

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 at their convenience. 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 Coronavirus pandemic to actively engage students.

Online learning is supported by various systems such as learning management systems (LMS), video conferencing platforms and student management systems (SMS). In this topic, we will cover these applications and highlight the security concerns over online learning platforms.

Learning Management Systems (LMS)

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 and programs. Learners can also pace themselves and access the course material from virtually anywhere. The learner's experience can also be personalized. Learning management systems store confidential data such as training content, student information and teacher information. This information is very crucial in the administering of online classes; therefore, it should be protected to prevent data breaches.

Examples of LMS

- TalentLMS
- Canvas
- Moodle
- Google Classroom
- Blackboard
- MookIT

Security concerns

Malware: Most learning management systems are vulnerable to malware. Malware is any malicious software used to gain unauthorized access into systems and networks to steal data or disrupt normal school operations. Malware can also be used to obtain confidential information such as passwords and usernames. Once an attacker obtains the username and password, they can use it to login and take over a user's account. Once logged in, most attackers will change the password, so that the legitimate user cannot access the learning management system.

Password guessing attacks: This is an attack where the attacker tries to guess the username and password by trying different combinations of usernames and passwords. If users have used weak passwords, it is easy for the attacker to correctly guess the password using some tools. This is a concern especially on the Moodle LMS.

Having explored some security concerns, it is important to explore the security features provided by the LMS to prevent unauthorized access and preserve confidentiality and integrity. If adequate security measures are not implemented in the LMS, cyber attackers can use the weaknesses in the LMS to steal or destroy sensitive information such as your course content and student information. Learning Management Systems also need to be updated regularly. This is because vendors continually release updates that address various security issues found in previous software versions. Lastly, ensure that you use strong passwords for your account. A strong password is harder to guess therefore attackers cannot gain access into your account.

To explore further the security features, here are some links:

Moodle LMS: https://docs.moodle.org/19/en/Security

Canvas LMS: https://www.instructure.com/canvas/security

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Student Management Systems

Student Management System or SMS is a management information system for learning institutions used to manage student data. These systems are also known as student information systems. Student data is very critical and sensitive in any learning institution, therefore, it must be managed properly and protected effectively. A leak of this data could damage the school's reputation and brand image.

Some of the key functions of SMS:

- Student information storage, including grades and attendance
- Faculty management
- Report generation
- Access portals for students and parents
- Enrollment or registration management

Examples:

- Blackbaud Education Management Solutions
- The PowerSchool Student Information System
- Infinite campus
- openSIS
- Gibbon
- School Time

Security Concerns

Malware: SMSs store very critical data for any learning institution. This data is very alluring to attackers; therefore, they will try to gain access into these systems using malicious software. Attackers are always trying to get you to click on a malicious link to download malware. For example, they will send spam emails trying to deceive you into clicking the links. Be very careful of any links sent to you by unknown sources. Only click on links from trusted sources.

Just as we had mentioned for LMSs, it is important to consider the security features offered by the student management system, otherwise, cyber attackers will exploit the SMS's weaknesses to gain unauthorized access. Cyber-attacks on student management systems could lead to data loss and data breaches, which can be very damaging to the reputation and brand of the learning institutions.

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Remember to use strong passwords to log into the student management system. Avoid sharing the password or writing it down, as students and unauthorized personnel can get a hold of these passwords and use them to access the system and modify their grades.

Video conferencing platforms

To support online learning, learning institutions also use various video conferencing platforms to hold live training sessions and webinars. These sessions usually simulate a physical classroom hence allow teachers to have real-time interactions with students, as well as foster active participation and engagement among them during remote learning. For instance, students are able to ask real time questions and the teachers can provide guidance. These platforms also enable audiovisual learning.

Some of the platforms used include:

- Zoom
- Microsoft Teams
- Google Meet
- Cisco WebEx
- Skype
- GoToMeeting

Security Concerns

Intruders: With videoconferencing platforms, intruders joining the call is a major security concern. Without proper implementation of security measures, unauthorized people can access and attend confidential sessions on video conferencing platforms. They mostly obtain links to virtual meetings from social platforms and can attend and disrupt the sessions. They can also obtain the links if you are using unsecured networks to join the meeting such as public WiFi. Unsecured networks allow attackers to intercept your information. Once they have joined the session, intruders can share inappropriate content and post links that lead to malicious websites or malware downloads on the chat feature provided by the videoconferencing platform. This makes videoconferencing platforms vulnerable to malware. We will look at various case studies of such incidents.

Intruders can also use your webcam to spy on you. This is because most sessions require you to have the webcam on. It is advised to only turn on the webcam when necessary and to ensure that it is disabled after the meeting is over.

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Privacy issues: Privacy is also a consideration in regard to video conferencing platforms. Most platforms have session recording options enabling teachers to record classes and share the recordings with students for future reference. However, educators must seek permission from parents to record and share the recorded sessions. When sharing the sessions, the links should be shared over secure channels

Educators must thus be keen to take advantage of the security and privacy controls provided by video conferencing platforms.

Teachers should also engage their students on video conferencing do's and don'ts.

These include:

- Ask your students to mute their mics. They can enable the microphone when they want to talk to the rest of the class.
- Advice students to join classes using their real names. This will enable you to properly identify and verify your students.
- Ask students to only share information related to the lesson on the chat.
- Let them know the consequences of breaking the classroom rules.
- Students should use the latest version of video conferencing solutions such as Zoom and Microsoft Teams.

Guidelines for teachers include:

- Do be careful about the documents or screens you share. This avoids accidental sharing of confidential data.
- Do ask students to use a laptop or a desktop computer to connect for a better user experience.
- Make sure to verify the student's identity to prevent intruders from joining. This can be done by enabling the 'Waiting Room'. Advice students to use their names instead of nicknames for easier verification. Don't allow them to rename themselves. This will enable better class management.
- Don't allow students to screen share unless it is needed for class presentations.
- If needed, remove students or parents who do not follow the classroom rules. This will maintain order.
- Disable private messages to foster transparency and easier management of the chat feature.
- Always reiterate the guidelines at the beginning of each class. This will engrain security into your students and ensure that they exercise caution while online.

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Additional guidelines:

https://www.campussuite.com/blog/tips-for-zoom-classroom-management-and-etiquette

http://www.lrc.columbia.edu/remote-teaching-dos-and-donts/

Before selecting technology to use for online learning, ask these three questions:

1. Is the online learning technology accessible?
2. How easy is it to use the technology?
3. Is the online learning technology safe and secure for school use?

In conclusion, security is an important element of online learning. Ensure that all the systems and applications you use as a teacher to deliver online classes are secure. Always explore and implement the security features provided by the application. This will protect you and your students against cyberattacks and protect your information.