CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Online Learning Attack Case Studies

Introduction

Image from Techcrunch

In March of 2020, many countries went into lockdown as one of the measures to curb the spread of the Coronavirus. This meant that brick and mortar schools had to close down and transition to online learning. Video conferencing platforms came to the aid of many schools during the transition period, with Zoom being one of the preferred options. With countless number of schools utilizing the video conferencing platforms, malicious attackers started to target these online classroom meetings to disrupt the sessions, share inappropriate content and even links to malicious sites. In the case of Zoom, this type of attack is known as zoom bombing.

Singapore

On Wednesday April 8th, an online Geography class proceeded as scheduled. However, two male hackers zoom bombed the class and proceeded to share obscene pictures to the teenage girls attending the lesson. The hackers went ahead to ask the girls to show their private parts on camera.

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Due to this incident, Singapore suspended the use of Zoom for online learning until the security concerns were addressed. The Ministry of Education encouraged teachers to learn and implement the security features that Zoom offers as well as to use updated versions of the Zoom application. To read more about the case, use this link.

Zoom has since then introduced security features to prevent Zoom bombing such as setting meeting passwords, waiting room features and disabling screen sharing for participants by default. When setting up classes, check the meeting settings to ensure that the security features are implemented.

Some of the settings to modify include:

- Disable "Join Before Host" so people can't cause trouble before you arrive.
- Enabling "Co-Host" so you can assign others to help moderate.
- Disable "File Transfer" so there's no digital virus sharing.
- Disable "Allow Removed Participants to Rejoin" so booted attendees can't slip back in.

To explore more security features provided by Zoom, use the link below:

Zoom security features: https://zoom.us/security

For other video conferencing platforms, use the provided links:

Microsoft Teams: https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide

Cisco WebEx: https://bit.ly/3gG9EDf

Google Meet: https://support.google.com/a/answer/9822731?hl=en

Moodle LMS

In 2017, a security researcher was able to hack into Portugal's University of Porto Moodle learning management system. He was able to access and manage user accounts, view hidden quizzes, download a full backup of the university's site as well as change grades. Luckily, the hacker did not share this data, but proceeded to contact the university and have the weakness resolved. Use this link to learn more about the case.

Moodle now separates user accounts to limit what a user can do on the site. For example, students have learner accounts hence they are only able to read the course content but they are not allowed to change it. Teachers have instructor accounts therefore they are able to create and add content for various classes.

To explore other Moodle security features, use the link below:

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

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Stanford University Data Breach

In 2019, Stanford students were able to view other students' college common applications and high school transcripts. Accessible documents also contained sensitive personal information including, for some students, Social Security numbers. Other data that was exposed included students' ethnicity, legacy status, home address, citizenship status, criminal status, standardized test scores, personal essays and whether they applied for financial aid. Official standardized test score reports were also accessible. This was caused by the use of an outdated content management system known as NolijWeb. A lot of learning management systems and student management systems are vulnerable to attacks that lead to data breach lead and data leaks. Stanford proceeded to notify the affected by the data breach as is required by the law. They also contacted the vendors to have the vulnerability rectified. Always update all your software to ensure that all the security weaknesses are rectified.

You can read further about the case using this link: Stanford Daily