CYBERSECURITY TRAINING FOR TEACHERS (CTT 1)

Week 2 Cyber –Attacks on Online Learning Platforms: Zoombombing & Security Breach Transcript

In this session, we shall look at the various cybersecurity attacks on online learning platforms. As a teacher, have you experienced any cyber security attacks while you're conducting your online learning sessions? Maybe yes or maybe no. When we learn about these attacks, you will be able to realize that you might have experienced these particular attacks.

The first attack we are going to look at is Zoombombing. Currently, most schools are using Zoom to conduct their online learning sessions. And you may ask yourself, what is Zoombombing? Zoombombing is a situation where an attacker accesses your Zoom class session without your authorization and disrupts learning. And how does Zoombombing takes place?

There are several ways of how zoombombing takes place. First, Zoombombing will happen if you do not secure your Zoom sessions with passwords. Normally, Zoom sessions have Zoom numbers or the session numbers. And in most cases, you will see that attackers keep on guessing this Zoom session numbers. And once they reach, say accidentally reach your session, and you have not secured their session with a password, they will easily enter your session and disrupt your learning.

Another way that Zoombombing takes place is a situation where you share your Zoom session number and the password to the public domain. Once you do that, when attacker get hold of this information, they will easily access your session and disrupt your learning. How do you protect yourself against Zoom bombing?

For you to protect yourself against Zoom bombing, first, avoid reusing the Zoom session numbers and passwords. Naturally as human beings, we are lazy. As a teacher, you may tell yourself that you have this class in the morning and another one in the afternoon. So there's no need of creating a new session for the afternoon class. You'll just reuse the morning session in the afternoon session. But that is very wrong. Because when the attacker might have gotten access to your morning class, they will easily compromise

your afternoon class. Therefore, it's important that for every new session, you create a new password and a new session number.

The second way you can protect yourself against Zoombombing is to ensure that you lock your Zoom sessions and use passwords always. So that in case an attacker comes in when the session is on, they will not access your session because you have locked it, and you have used a password to secure your session.

The third way you can protect yourself is avoid sharing a Zoom session credentials on the public domains. For example, do not share them on Facebook or Instagram. But rather it's advisable that you text every student individually and tell them the Zoom session number and the Zoom password.

Fourthly, ensure that you use the Zoom security features. For example, on Zoom, we have a waiting room. When the students are logging in, or your participants are logging in into our session, they will be kept at the waiting room. From the waiting room, you will be able to verify that these are the correct people, or these are the right students to access your lesson. And in this case, there will be no disruptions. Basically, that's how you protect yourself against Zoombombing.

Let us look at another attack, which is security breach or data breach or information breach. And how does security breach occur or what is a security breach? A security breach is a situation where an intruder gains access to your system without your authorization. And once they gain this access, they compromise your information. They may expose it or alter your information. That is a security breach.

We have three common ways of how security breaches occur. The first way is through hackers. Hackers gain unauthorized access and maybe this is facilitated through phishing. They gain unauthorized access into our system. Once they gain this unauthorized access into your system, they compromised your information. They might even encrypt it or alter your information, or they might copy it and expose it to the public domain.

The second way of how security breach takes place is through human error. And what do I mean by human error? Human error is a situation you as a teacher or even me, accidentally sends mails or information to

the wrong person who is not authorized to access that information. Or maybe lose my information, or my electronic gadgets; that is my mobile phone, or even my mobile gadget. And once I lose these gadgets, the information that is stored in these gadgets can be easily accessed by unauthorized people, which leads to a security breach.

Another way of how a security breach can occur is through unauthorized use. For instance, as a teacher, you might have been authorized to access the student's exam records, but you're not authorized to alter anything on those records. But as a teacher, maybe you see that your students have performed so poorly. So you end up changing their exam grades, so that the school head can see that as a teacher, you have performed well. In the course of altering those records, you are causing a data breach.

How do you protect yourself against data breach? One way of protecting yourself against security breach is by enhancing your system login credentials. How do you enhance your system login credentials? For example, you might apply the two factor authentication, whereby once you login into the system, it prompts you on your mobile phone. It gives you a code, which you have to input that code first for you to access the system. Or you might mix passwords with biometrics, whereby you use your fingerprints, or even your iris to log in to the system.

Another way of how you can protect yourself against security breaches is to use different passwords on different accounts or different systems. And when you do that, when one of your accounts is compromised by an attacker, the attacker cannot use the same login credentials from this account to compromise another account, or another system. It's also advisable that you use secure passwords. In the coming week, you will learn how to create secure passwords.

You are also advised to protect your devices, especially the mobile devices, because these devices can be easily stolen, or you can easily lose them and when you lose them, you don't know in whose hands they're going to land in. They may land in the hands of a criminal who will now gain unauthorized access to information which leads to a security breach.

CYBERSECURITY TRAINING FOR TEACHERS (CTT 1)

And lastly, you are advised to always backup your information and secure your backup. In case you lose your information, or your gadgets, you can easily get your backup information and continue with your business as usual. This brings us to the end of this in this video. In this video, we have looked at two attacks. That is Zoom bombing and security breach. In the next video we are going to look at more attacks.