CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Security Attacks on Online Learning Platforms: - Classroom Hijacking and Security Breach

Types of cyber-attacks on online learning platforms

1. Classroom hijacking or zoom bombing

Classroom hijacking/*Zoombombing* is an unwanted, disruptive intrusion, by internet criminals into a zoom class session. In the recent past, there have been various reported incidents of zoom bombing.

How does classroom hijacking/zoom bombing occur?

There are various ways of how zoom bombing takes place

a. Zoombombing takes place when the teacher (host) does not protect the zoom session with a password. In this case, just by flipping a couple of numbers, the attacker could potentially get lucky and access someone else's online class session without authorization
b. Zoombombing may also occur when the teachers and the students share their zoom class password to unauthorized individuals.

How to protect yourself against zoombombing.

a. For teachers to be secure when holding zoom classes, they should avoid re-using zoom session ID and password with every call.
b. Teachers should ensure that Zoom's security features have been enabled on the meetings they are setting up. These features include: the "waiting room" feature which prevents illegitimate users from joining a call before they've been screened by the teacher (host).
c. Teachers should ensure that the "share screen option" is only available for authorized users.
d. Teachers should ensure that they mute every student's microphones and lock the meeting when all the students have joined to prevent break-ins.
e. Both teachers and students should avoid posting the zoom class session links on public platforms.

2. Security breach

According to your specific country, what are the available channels for reporting cybercrime?

A security breach is an incident that results in information being accessed without authorization. It may lead to exposure of confidential or protected information. In online learning platforms, security breach involves the loss or theft of the staff and students' records, exams, and other sensitive information.

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Security breach comes in many forms such as hacking, insider breach, physical document loss, portable device breach, stationary device breach, or unintended disclosures.

How do security breaches occur?

A security breach occurs when an intruder gains unauthorized access to an organization's protected systems. Below are some of the ways it can occur:

a. **Criminal hacking.** Cyber criminals obtain staff's or student's credentials by stealing, hacking into online learning systems, or buying them on the internet. Once a cyber-criminal has a user's login credentials, they can perform any number of nefarious activities, but it usually boils down to extracting information to commit fraud or sell on the dark web, or to launch further attacks, such as phishing scams.

b. **Human error.** More than half of security breaches on online learning platforms happen as a result of human error. The most common errors involve sensitive information being sent to the wrong person. This might involve sending an email to the wrong person, attaching the wrong document, or handing a physical file to someone who shouldn't have access to the information.

c. **Social engineering.** Social engineering is another common way through which security breaches occur. In this case, the attacker simply acts as though they belong, for instance, they may pretend to be legitimate students or even parents so that they can be given access to the system. Once attacker gains access to the system, they gather sensitive information, commit fraud, sell the data, and vandalize the system.

d. **Malware**. Malware can be used by cyber criminals to commit various security breaches, for example, they may use spywares and key loggers to steal system passwords and other sensitive information. A spyware, just like a spy, secretly observes activities on your computer and sends these observations to the criminals. On the other hand, key loggers are used to monitor the activities on your keyboard (keys pressed) and send this information to the person monitoring you.

e. **Unauthorized use. Schools** consistently overlook the threat their employees pose, but most security breaches on online systems are caused by a member of staff using information improperly. There are two main ways this happens. The first is privilege abuse, in which teachers misuse information they've been given legitimate access to. This isn't necessarily

for malicious purposes. The teacher might have stumbled on the information accidentally, which can happen if the school doesn't set up appropriate access controls.

Alternatively, the teacher could have ignored access guidelines. This can happen when, for example, the teacher alters a document without following the correct procedure.

The second common type of privilege misuse is data mishandling. This occurs when sensitive information is copied, shared, accessed, stolen or otherwise used by a teacher who isn't authorized to do so.

How to protect yourself against security breaches on online learning platforms.

a. **Enhance school login requirements**. Use strong passwords with uppercase and lowercase letters, non-sequential numbers and special characters.
b. **Use different passwords on different systems/accounts**. If one account is compromised, cybercriminals won't be able to easily access your other accounts.
c. **Use secure websites**. Look for "https" in the web address. It indicates a secure - connection.
d. **Install updates**. Always update your computers and mobile devices with the latest versions of operating systems and applications. Updates sometimes contain patches for security vulnerabilities.
e. **Be proactive**. In case a security breach happens, it's important to know what personal data was exposed and what you should do to help protect yourself. This might include changing passwords on the online learning system.
f. **Protect personal devices** – While mobile devices offer great benefits, they create risks of infection when unsecured devices are connected to the school's online learning system.
g. **Back up your data** – It is a good practice to consistently back up your data to protect against a system failure.