



ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Cybersecurity Threats, Vulnerabilities, and Risks

Introduction

In this module you will learn about the most important cybersecurity challenges and mitigation techniques that are relevant to online learning platforms. The module will cover the security threats on various online learning platforms like Moodle, WebCT, Blackboard and social media. Given that the main elements of online learning platforms are sharing of information, collaboration and interconnectivity, it is important to equip yourself with the knowledge on how you can protect yourself and the students on online learning platforms against data manipulation, fraudulent user authentication, and compromises in confidentiality.

Cybersecurity Threats, Vulnerabilities, and Risks

In today's world, most learning institutions have shifted to online learning and they collect, store and share valuable, sensitive data on their students and staff members. This data ranges from allergies and learning disorders to grades, examinations and course material. As a result of this, just like other organizations, schools have become vulnerable to cyber-attacks. Therefore, data and protecting that data are critical considerations that should be taken into account. Schools should ensure that their information is secure and if they can't keep it safe, they will lose their reputation and credibility. With this consideration, as the teacher, how confident are you when it comes to your school's information security?

In order to have a strong handle on data security issues that may potentially impact your school, it is important to understand the relationship between three central components: threat, vulnerability, and risk. Although these technical terms are used interchangeably, they are distinct terms with different meanings and implications.





ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Examples of vulnerabilities

1. **Outdated Software.** An outdated software normally has weaknesses, thus, the vendor releases security updates to cover them, for instance, Microsoft normally releases periodic Windows updates to patch the vulnerabilities. Vulnerabilities in online learning systems occur when an outdated software has not been updated to include the latest software updates.
2. **Removable Media.** Media devices that can be connected to computers, such as flash disks, external hard disks, CDs, and DVDs also pose challenges to online learning platforms. These devices can be easily stolen or corrupted with malicious software that may infect the computer.
3. **Weak authentication.** Authentication is the process of providing proof that you are who you claim to be e.g. providing username and password when logging on Moodle. When authentication credentials are compromised or weak, user identities can be stolen and used to gain unauthorized access to the online learning system and compromise it. For example, when you use weak passwords (such as date of birth, children's name, and pet names), criminals can easily guess and use them wrongfully.
4. **Humans.** The weakest link in any system is the human element. In this case, both teachers and students can easily expose sensitive data and create access points for attackers.

Examples of threats

1. **Phishing.** Phishing is the act of sending an email falsely claiming to be from a legitimate organization with the intention to deceive the recipient into divulging sensitive information like passwords, student records, and exams, after directing them to visit a fake website.
2. **Malware.** Malware is a collective term used to denote a number of malicious software, including viruses, ransomware and spyware. This malicious software interferes with the normal functioning of the computer and the online learning system. They also corrupt and steal electronic records. There are various ways that computers can become infected with this malicious software, for instance a user might download a piece of malware disguised as a legitimate software, email attachments or links.

Examples of risks

Risks include financial losses for schools, loss of privacy of student and staff information, school's reputational damage, legal implications, and even loss of life.