



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Introduction to Cybersecurity

Objectives

- Understand cybersecurity and its importance.
- Contextualize cybersecurity for online learning.

Introduction

In this module, we will define cybersecurity and explore its importance in our lives. Since we are increasingly incorporating technology to support online learning, we will also look at learning management systems, student management systems and video conferencing platforms and their impact on cyber security. Lastly, we will explore various cybersecurity laws and organizations that govern cyberspace.

Technology has greatly impacted our lives in terms of how we interact, how we work, how we learn and even how we teach. For example, through technology, you are taking this course at your convenience. We are able to teach using video conferencing platforms such as Zoom and Microsoft Teams. Class textbooks are now available online as digital copies. Exams can also be administered online. This positively enhances distance and online learning, extending the education reach to remote and rural areas.

Despite the life changing impact of technology, it has also introduced security concerns. Cyber-attacks in learning institutions have been accelerated by the transition to online and distance learning, hence the need for cybersecurity.

What is cybersecurity?

Cyber security is the practice of protecting systems, devices, networks, programs and information from digital attacks. Its main function is to protect the information stored in these systems from modification and unauthorized access. Cyber security is a continuous process; therefore, we have to bear security in mind while interacting online.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

What is Cyberspace?

Cyberspace is the global interconnected digital technology. It is the virtual environment in which online communication occurs. It is made up of systems, devices, networks, applications and information. When you connect to the internet on your mobile phone or on your computer, you become a part of the cyberspace. When you share your stories on social media platforms such as Facebook and Instagram, you also are a part of cyberspace. When you are teaching a class via Zoom, or Google Meets or any other platform, you are using cyberspace. The cyberspace allows us to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business, learn and teach too. The cyberspace is virtual, and thus not geographically confined because devices are interconnected globally. This makes it a lot more difficult to protect because threats can emanate from virtually any part of the world. The best way is to protect ourselves by securing our devices and exercising caution while interacting online.

Why is Cybersecurity Important?

So why should you care about cybersecurity? As we had already mentioned that the main objective behind cybersecurity is to protect information from modification and unauthorized access.

What kind of information do we need to protect?

- Financial data - fee payments, payroll information
- Personal information - name, employment history, residential addresses, contact information, health information
- Student records - performance grades, health information, parent information
- Employee records
- Credit card information
- Intellectual property - training content, books

Failure to protect the school's assets such as computers, laptops, and learning management systems, may lead to cyber-attacks. A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's information and computers. You will learn more about cyber-attacks in the next module.

Cyber-attacks have devastating effects on organizations and clients. These include:



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

- Financial losses - criminals can get hold of your financial information and empty out your accounts. Criminals can also lock your school's data storage and demand a financial ransom for the school to regain access to their files.
- Damage of brand image and reputation - You have heard of people who have been hacked and the criminals shared damaging information about them on social media. In learning institutions, a leak of student confidential data can damage the school's reputation.
- Loss of confidential data such as student records. Imagine if your laptop was compromised, and the attackers behind it shared this information; both your students and their parents would be devastated. This could also damage your reputation and that of the school.
- Identity theft - Hackers can impersonate you and can land you in debt by taking loans. They can also damage your relationships.
- Inconvenience normal business operations - As the security personnel are trying to rectify the cyber-attacks, operations are disrupted. For example, if hackers prevent access to the school's learning management system, students are unable to access the content and classes are disrupted.

It is important to mention that cybersecurity is a collective effort, therefore, it is our responsibility to make sure that we are protected against these cyber-attacks. Cyber attackers target people using attacks designed to trick and deceive them into divulging confidential information or click on malicious links. This is known as people hacking or social engineering. You could be the weak link that lets attackers into your organization's network. It is thus very important to learn about cybersecurity through an awareness program such as this course that you are taking. That way, you are able to protect yourself and your organization from cyber-attacks.

To explore cybersecurity further, we will look at cybersecurity principles.