



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Week 1 Introduction to Cybersecurity Transcript

Hello, and welcome to this first week of the cybersecurity training for teacher's course. My name is Patricia Musomba. And I'll be your instructor this week. During this week, we'll define cyber security and explore its importance in our lives. We'll also look at various learning platforms such as learning management systems, and video conferencing platforms. Lastly, we'll also look at various cybersecurity laws and regulations.

Before we look at cyber security, let us first look at how technology has changed our lives. Technology has changed how we interact, how we work, how we learn, and even how we teach. For example, through technology, you're taking this course at your own convenience. Through technology, we're also able to teach online using video conferencing platforms such as Zoom. Exams are now even administered online, and teachers and students can access material via learning platforms. This has positively enhanced distance and online learning therefore, extending the reach of education into rural and remote areas. Despite the life changing impact of technology, it has also raised some security concerns. Cybersecurity attacks are now on the rise due to the incorporation of online learning in learning institutions. With this in mind, let us now look at what cybersecurity is.

Cybersecurity 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 for modification and unauthorized access. It is important to remember that cybersecurity is a continuous process and therefore we should bear it in mind and every single time we're online. To properly understand cybersecurity, we also need to understand the cyberspace.

The cyberspace is the global interconnected digital technology. It is the virtual environment on which online communication takes place. The cyberspace enables us to interact online on social platforms, as well as do business, and teach as well as learn. It is made up of systems, devices, networks, as well as information. For example, when you connect to the internet through your mobile phone or your computer, you become a part of the cyber space. In addition, when you're sharing stories online via social platforms, such as Facebook, and Instagram, you also are part of the cyberspace. The cyberspace is virtual and therefore it is not geographically confined. Because it is a global network, it is very difficult to actually secure the whole network. This is because attacks could come from virtually any place in the world. With an understanding of cybersecurity, let us now explore its importance.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

The main aim of cyber security is to secure the information. But what kind of information needs securing, we're looking at information such as financial data. This includes things like fee payments, banking details as well as payroll information. We also have personal information. This information includes employment history, residential addresses, contact information, as well as health information. We also have student records, that is performance grades, health information as well as parent information. Another type of information that we need to protect is credit card information. This is because when an attacker has your credit card data, they are able to pay online using your card, they can also impersonate you.

Lastly, we also need to protect intellectual property. This is data or other content that you have created on your own and you would not want used without your explicit permission. For example, we have books that you created and also training contents that you have created for your students.

What are some of the consequences of not protecting yourself and your information? Failure to protect your data assets, such as your computer, your mobile phone could lead to cyberattacks. A cyberattack 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. Cyberattacks usually have very devastating effects on the person's computer or the organization's network.

Let us look at some of these effects. Cyberattacks can lead to financial losses. For example, when criminals get a hold of your credit card information, they can use it to pay for things online without your permission. They can also lock your school's data and ask for a ransom in return. Thereby, the school will spend a lot of money to gain access back to the data.

Cyberattacks can also lead to damage in the brand reputation and image. I'm sure you've heard of people who have been hacked and the criminals have shared very damaging data about these people online. These days can be very embarrassing, and can damage your reputation. For schools, when this information is shared online. It can also damage the school's reputation and hinder any enrollments of students.

Another effect of cyberattacks is identity theft. When hackers have enough information about you, they can easily impersonate you, and can even go to an extent of taking loans in your name. Lastly, cyberattacks usually inconvenience normal business operations. This is because, as the IT



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

personnel is trying to rectify the situation, normal operations are disrupted. For example, if hackers prevent access into the learning management system, students will be unable to access the content and classes will be disrupted for the day.

Having looked at what cyber security is, and the impacts or other the consequences of cyber-attacks, we need to understand whose responsibility it is to implement cyber security. It is important to mention that cyber security is a collective effort. Therefore, it is your responsibility and mine to make sure that we are protected against cyberattacks. Cyber attackers usually target people by using attacks that are specifically designed to deceive you into divulging confidential information. They also try to trick you into clicking malicious links. This is usually known as social engineering and you will explore this much later.

It is therefore very important for you to learn about cybersecurity through an awareness program or through a course such as this one that you are taking. That way you will know about cyber security, you will know about the attacks and how to protect yourself.

And with that, we have come to the end of this video. In this video, we defined cybersecurity and the cyberspace; we also explored its importance. We then looked at the consequences of cyberattacks, and how it is your responsibility to make sure that you're protected.