CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Cybersecurity Threats, Vulnerabilities, and Risks Transcript

Hello everyone. I am Linda Mwibanda. Your instructor for week two. In week two, we are going to learn about cyber security threats and mitigation. Currently, we see that most schools have shifted their learning to online whereby teachers create their content using online platforms. They teach students using these online platforms, administer exams store their content online. As a result of these, schools have become vulnerable to cyber security attacks. For us to be able to protect ourselves against cyber security attacks on online learning platforms, it's important that we learn about the cyber security components.

We shall start by looking at three central components of cyber security. This is vulnerability, threat and risk. Although in many cases, most people use these terms interchangeably but these times are very distinct and they each hold a different meaning. Now, what is vulnerability? Vulnerability is a known weakness in the system that can be exploited by a hacker to cause harm. What are the various examples of vulnerabilities?

First, we have outdated system or software. When your system is outdated, it will have some security issues which can be easily used by an attacker to cause harm. For instance, Microsoft Windows releases system updates periodically and these updates are used to patch up the system vulnerabilities. They have security features which patch up the system vulnerabilities that can be exploited by a hacker. Therefore, it's important that whenever an update is released, you make sure that you patch up your system according to that particular update.

Another example of vulnerability is removable media. Removable media are things like flash disks, external hard drives or CD-ROMs. How are they vulnerable or how do they cause cyber security vulnerability? You know, when you have your flash disc and you put it in a machine that is affected with a virus, you can easily copy files, those affected files and transfer it to another machine. When you're transferring those files, you are also transferring the virus.

At the end of it all, you will realize that the entire school is affected by this malicious software and that is a virus. When the machines are affected, you'll not be able to access your files because your files will be corrupted. Therefore, it's important that you do not use this removable media to transfer your documents

or your files. Another reason why we say removable media is a vulnerability is because you can easily lose this removable media. For example, you can easily lose your flash disc and once you lose your flash disk, it may end up being accessed by a person who is not authorized. Once this unauthorized person accesses your flash disk, they will copy whatever content is stored in that flash disk.

Another example of system vulnerability is weak authentication. What do I mean by weak authentication? Weak authentication is a situation whereby you have not secured your systems with proper passwords or your systems have these default password settings. For example, it has admin as the username and admin as the password. With this, the hacker can easily log in to your system and compromise your system.

The last vulnerability on online learning systems is the human being and why human beings? They always say human beings are the weakest link in any system. Why are humans the weakest link? Because naturally, human beings are susceptible to tricks. Someone can come and lie to you so that they gain access to the system or gain access to their confidential information.

Another central component of cyber security is a threat. What is a threat? A threat is something that can potentially cause harm to your system and what are various examples of threats? First, we'll have phishing. What is phishing? Phishing is not this fishing where you go to the Lake and get fish. It is a situation where you receive an email which states that it's coming from a legitimate organization. And in most cases, these emails they tend to ask you for confidential information or for personal identifiable information. Therefore, when you just give this information without verifying the source, you might be causing a cyber-security attack.

Therefore, it's important that when you receive any email requesting you to submit any confidential information, make sure that you call the person or the organization that has sent you the email to verify whether they are authorized persons. Another example of a threat is a malware and a malware is a collective term to mean malicious software. Malicious software comprises things like viruses, we have things like ransom ware, we have things like adware, and we have things like spyware.

You may be wondering what is a virus, what is an adware and what is a spyware? A virus is software that replicates itself from the word virus. Once this virus has affected your system, it corrupts your files in such

a manner that you cannot access them. What is an adware? From the word advert, you get the term adware. It's a malicious software that comes in form of an advert. Sometimes when you're accessing the internet, you see those flashy adverts maybe telling you click here and you'll win a million. That is an adware. Once you click on it, that malicious software will embed itself on your system. What it does, it also corrupts your file.

Another type of malicious software is spyware. From the term spy, what does a spy do? A spy snips around for information. Therefore, these malicious software, these pirates, they also sniff around in your system for information. Once they get this information, they send it to the attacker and the attacker can use this information to compromise you. Therefore, it's advised that you always use antiviruses to protect yourself from these malicious software.

Let us look at the last component which is risk. What is a risk? A risk is the likelihood of a loss or damage. Therefore, when you have a vulnerability and you have a threat, when you combine the two, you get a risk. Once the vulnerability is exploited by the threat, you end up losing your documents or you end up even losing life because when people get your information, they might track you and do you harm or you may lose your credibility as a school.

When your credentials or your confidential information is exposed to the public domain, you will lose your credibility and you may end up losing even your students from registering with your school. Now this marks the end of us learning about the central components of cyber security, which were vulnerability, threat and risk. In the next session, we shall look at various cyber security attacks on online learning platforms.