CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Cyber Attacks on Online Learning Platforms: Identity theft & Ransomware (Transcript)

In this video, we shall continue learning about more cybersecurity attacks on online learning platforms. We shall start by looking at identity theft as one of the cybersecurity attacks on online learning platforms and now what is identity theft? Identity theft is a situation where an attacker uses your personal identifiable information to compromise you or compromise the system and how does it happen?

One of the ways of how identity theft occurs is through phishing. In phishing is where you get an email requiring you to submit your personal identifiable information. For example, the attacker sends you a form requesting you to fill in that form with your personal identifiable information. Once you fill in that form and send that information, you're not sending that information to the legitimate organization as the mail has said but instead, you're sending that information to the attacker who will now get access to your personal identifiable information or your confidential credentials. Once they get that information, they will masquerade themselves to be you and compromise you or compromise the system.

Pharming is also another way of how identity theft occurs, and in pharming is why your browser is compromised by a virus or is hijacked without your knowledge. Once your browser is compromised, when you type in your school's legitimate website, it redirects you to a fake site that looks like your school's original site. In this case, the cybercriminal collects your personal identifiable information, which you might have entered on that website.

Malicious software is another way of how identity theft happens. In this case, the attacker uses malicious software like spyware and keyloggers. Spywares just like the word spy come and snoop around for information. Once they get access to this confidential information, they send it to the attacker.

Another way is keyloggers. Keyloggers monitor the activities of your keyboard. When you type in spacebar, the keylogger is able to know that this is a spacebar. When you will type in any letter on your keyboard, the keylogger is able to know that this is a specific letter or a particular letter. Once they collect that information, they will send it to the attacker who will now filter in through that information and be able to identify your personal identifiable information and use it without your authorization.

Discarded computers or mobile devices are another weak point of how identity theft occurs and how does it happen? When your machine is spoilt or your machine is outdated and you want to dispose it, it's important that you wipe away all your personal identifiable information from that machine. If you do not do that, the attacker might easily get access to that information and use it against you.

Those are the various ways of how identity theft happens. Now how do you protect yourself against identity theft? There are various ways of how you can protect yourself against identity theft. First, build strong passwords. When you build strong passwords on your systems, it's not easy for an attacker to guess your password or to gain unauthorized access into your system.

Avoid over sharing your personal identifiable information on social media. Nowadays, you realize that most of people or most of us, we post our mobile phone numbers, our email addresses, where we come from or where we are currently staying on social media. When these attackers gain access to this information, they will be able to steal your identity and compromise you. It's important that you educate your students and your colleagues on the importance of using strong passwords and maintaining general online hygiene, whereby they don't over share the information or they do not visit sites which are not secure.

Another way of how you can protect against security breach is establishing protocols. For instance, when I am a teacher in grade one, I should not access grade two exams or results or information because I might be tempted to compromise that information. You are also supposed to monitor access control. Whoever accesses that information should be monitored. Or for example, when you're holding a Zoom class, make use of the waiting room so that you are able to monitor who is accessing your class session. This will help you to avoid being compromised or identity theft.

So, it's of good manner if you always take good care of your personal devices, especially these mobile devices. Lastly, be careful with emails which are requesting you for personal identifiable information. When you receive such emails, always make sure that you call the organization or the person who has sent you the information, so that you're able to verify that actually it's this person who has sent you the

information. Otherwise, you will end up sending your personal identifiable information to cyber security attackers.

The last type of security attack we are going to look at is ransomware, and ransomware from the word ransom is malicious software which attackers use to encrypt all your information on the system. Once they encrypt this information, they will request you to pay a given amount of fee so that they can give you access that will decrypt this information. These threats come with short term deadlines and in case you fail to meet the first deadline, the amount of ransom keeps on rising. So, it puts you in a panic mode which will make you to pay up so that you can be given access to your information or your system.

How does ransom ware attack take place? Ransomware attack happens as a result of risky online behavior. What do I mean by risky online behaviors? Naturally, we as humans we like free things. In the process of wanting free things when we are online, we end up on clicking pirated websites for entertainment or for downloading music and videos. These pirated entertainment websites are where most hackers embed their malicious software's there.

System vulnerability is another way of how ransomware attack can take place. When you have not updated your system or installed an antivirus, malicious software can easily spread through the system and compromise you. Therefore, it's advisable that you always patch your systems and install antiviruses on your systems.

The last reason that can cause a school to be compromised by a ransomware is cost. Most schools do not have a budget for cyber security. This causes you as teachers or the students to use free software from online and you know there's nothing like free. This free software are full of viruses or ransomware. Therefore, it's important as a school to have a budget for cyber security or buy authentic software, which you can use on your system.

How do you protect yourself against ransom ware? First, train all the students or the teachers on the importance of cybersecurity. When you do that, they will understand that it's not advisable to visit

websites with pirated content or they will know that when they receive an email, they will verify that this email is from a legitimate source.

Secondly, perform regular system updates. When you perform regular system updates, you will be patching up whatever system vulnerability that is on your system. When you regularly update your system, it prevents the ransomware or any other malicious software from spreading through your system.

Lastly, backup all your information then secure your back up. In case you are hit up with a ransom ware, you are able to retrieve your backed-up information and continue with your learning as normal. This brings us to the end of learning about cybersecurity attacks on online learning platforms. Some of the attacks that you have learned in these lessons are Zoom bombing, identity theft, security breach, and ransom ware. I believe that you have mastered all the ways of how you can protect yourself against these particular attacks.