CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Security Attacks on Online Learning Platforms: - Identity Theft and Ransomware

Types of cyber-attacks on online learning platforms

1. Identity theft/masquerading

Identity theft affects millions of online students and teachers every year and occurs when a fraudster steals the student's/teacher's identity by gaining access to their personally identifiable information (PII) to commit fraud. Student's/teacher's PII can include names, emails, passwords, identity numbers, contact numbers, addresses, birth dates, course details, and school information.

How online identity theft happens

As teachers and students share their personal information on online learning platforms, social media and other digital channels, they may be putting that information at risk of falling into the wrong hands. Fraudsters use high-tech and other ways to steal digital data:

a. **Phishing** occurs when cybercriminals send emails purporting to be from a financial institution or other trusted organization, trying to trick you into opening attachments or clicking on links and providing your PII. Ignore unsolicited emails and online requests for information. If you want to visit, say, your school's website to provide information, type in the URL rather than clicking on an emailed link.

b. **Pharming** occurs when your browser, compromised by a virus, is hijacked without your knowledge. You type a legitimate website URL into the address bar, but you're redirected to a fake site that looks legitimate. Cybercriminals are able to collect any PII you may type into the illegitimate website.

c. **Malicious software.** Fraudsters may try to trick you into downloading "malware" that can attack your computer and, possibly, reveal your PII for instance spyware. Consider purchasing online security software for your computer such as Bitdefender, and keep your operating system and software applications up to date.

d. **Weak passwords** used for both social and financial accounts can leave you vulnerable. Strive to use unique, long, and strong passwords for each of your accounts. And when possible, activate multi-factor authentication, which requires you to enter both your log-in credentials *and* a secret code sent to your smartphone or other device before giving you access to your account.

e. **Discarded computers and mobile devices** that haven't been wiped of your PII can be another point of access for a cyber-criminal.

How to protect yourself against identity theft

There are many reasons students are especially vulnerable to identity theft; they are young, generally inexperienced with technology, and usually don't look through their entire online profiles. Many parents have their children learning online, but they don't keep track of their daily transactions. Consequently, parents don't know which transactions might be fraudulent. Students, parents, teachers, and schools should use the following tips and strategies to reduce the risk of student identity theft.

a. **Build strong passwords**: Make passwords stronger by taking out vowels and adding in special characters. Avoid using the same password on every website.
b. **Don't overshare on social media**. Identity thieves can mine social media posts for clues to account security questions and passwords.
c. **Educate your child about passwords**. Share techniques to build strong passwords, caution them to never share passwords with friends, and keep personal information like driver's license number and social security number private.
d. **Establish security protocol**. Each employee should understand his or her responsibilities for complying with security guidelines. Trainings should be conducted on a regular basis.
e. **Monitor access control**. Ensure that users are who they claim to be, and that they have the appropriate access to system. For example, when holding a zoom class, make use of the "waiting room" feature to enable you verify the genuineness of the students.
f. **Secure mobile devices**. Smartphones, laptops, tablets, and iPads with sensitive data should be secured with strong passwords.
g. **Be careful with email**. Teachers and school staff should be wary of sending sensitive information over email. Data that is being transferred should be encrypted and desensitized prior to sending.

2. Ransomware

Ransomware is a type of malicious software that encrypts data on a computer making it inaccessible to the owner. The attackers normally demand for extortionary payment from their victims to make the data accessible. The demand often includes a series of deadlines for payment - each missed deadline leads to

a higher demand and threats of destroying the data. If the victim doesn't pay up, the attacker makes the data permanently inaccessible.

How ransomware attack happens

Schools present a tempting target for ransomware attacks for several reasons.

a. **Risky online behaviors**: students and teachers often engage in risky online behaviors that expose them to ransomware attacks, such as treating email attachments without appropriate wariness, and visiting websites trafficking pirated content.

b. **System vulnerabilities**: the highly open and interconnected nature of school systems open up multiple points of malware infiltration: find a weak link (unpatched systems), and ransomware can spread quickly from student to faculty to staff PCs and servers.

c. **Cost**: cost pressures have made it difficult for some institutions to fund IT security investments; the education sector generally lags behind industries like finance, retail, healthcare, energy and government, in resilience of its technological infrastructure. This combination of factors has made education the most popular target for ransomware attacks.

How to protect yourself against ransomware

In the face of this rapidly growing threat, educational institutions can take some decisive steps to protect their systems from the operational disruptions and high costs of successful ransomware attacks.

a. **Train all students and staff:** start educating students and staff to be wary of the email links they click on, websites they visit, and attachments they open.

b. **Regular system update:** good security hygiene measures remain important, like separating networks to make it harder for ransomware to spread from system to system, keeping anti-malware software (such as antivirus) up-to-date, and keeping operating systems and applications updated.

CYBERSECURITY TRAINING FOR TEACHERS (CTT)

c. **Backup everything and protect your backups:** institute a rigorous backup regimen and keep multiple copies of critical data. Routine, frequent backup remains the most foolproof defense against ransomware: if your systems are compromised, you can simply identify the onset of the attack and restore your systems from clean backups created before the incursion.