ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT)

Cybersecurity Risks in Emerging Technologies

As you learned in CTT1, cybersecurity risk is the likelihood of exposure or loss as a result of cyber-attacks or data breach in your organization. Schools are becoming more vulnerable to cyber threats due to increasing reliance on emerging educational technologies. The ongoing pandemic has changed the mode of learning for schools, colleges, and universities the world over. With physical buildings closed, most educational institutions have moved to remote learning. For the majority, the transition from physical to online model of learning has happened too quickly. Without proper time to vet potential risks, the networks are exposed due to the deployment of new technologies and apps. Furthermore, risks can also increase because students and educators are not always properly trained to use the new tech.

Further complicating matters, many educational institutions simply do not have the budgets to overhaul their technology solutions in the face of such a pandemic. As a result, some institutions are lured by free tools and apps for online learning, most of which come laden with inadequate privacy controls, user tracking, inappropriate promotional content, and sometimes malware, all of which elevate the cybersecurity risks.

What are the major and common Cyber Risks and Threats in emerging educational technologies?

With emerging educational technologies becoming a new normal, cybercriminals are busy finding new ways to leverage techniques like phishing, ransomware, social engineering, and more to pull off attacks. Below are some of the most critical risks to be addressed to safeguard users (teachers, students) and data.

1. **Remote access:** With distance learning taking over physical schooling, students and teachers need access to online learning tools mostly located in the cloud file-sharing applications, email, apps, and they sometimes need to remotely access resources on the school network. At the same time, administrative and IT staff working from home may need access to systems and documents located on the school network as well. If remote access is not secure, hackers can sneak in and take control of the entire network. Deploy a virtual private network (VPN) that offers secure remote access to your users and protects all data that flows in and out of the VPN by encrypting it.

Students and school staff may bring their own devices and connect them to the school network, some of which may be unpatched and running risky applications, giving easy access to attackers. To counter this, ensure only white-listed apps run on the network and that only authorized devices can access the network. With complete application visibility and control, you can identify all the applications on your network including shadow IT (also known as embedded IT, fake IT, stealth IT, rogue IT, feral IT, or client IT) and data at risk. This allows you to control the apps and apply user-based application controls.

2. **Access to sensitive data:** Educational institutes are treasure troves of valuable information that can be sold on the dark web. Personal data of students, teachers, alumni, and administrative staff, along with sensitive data relating to a school's research and intellectual property can make a hacker very rich by selling it or ransoming it. It is critical to ensure access control to sensitive data by enforcing access based on user identity, allowing authorized users access to only what they need to do their jobs. You can protect sensitive data, research, and other critical resources by allowing access to only those who are authorized, with two-factor authentication (2FA) support for access to key system areas.
3. **Malware:** The adoption of emerging educational technologies like mobile/remote learning means many of the devices connecting to the school network are BYOD (Bring Your Own Device). As a result, mobile devices are being utilized by both educators and learners, with new devices pervading schools across the world. Many of these new and advanced mobile devices (such as iPads, new Android phones, tablet devices, and portable Internet access systems) are launched daily with upgraded versions of operating systems; these are ripe for malware infections and ready to infect school's network system. These malware infections include viruses, worms, Trojans, rootkits, spyware, crime-ware, and adware.

   Additionally, it is difficult to know whether the devices and applications used are updated with patches and if the antivirus is current. Unless such remote devices are connecting via a VPN, you will need to ensure they are secure before they can access resources on the school's network.

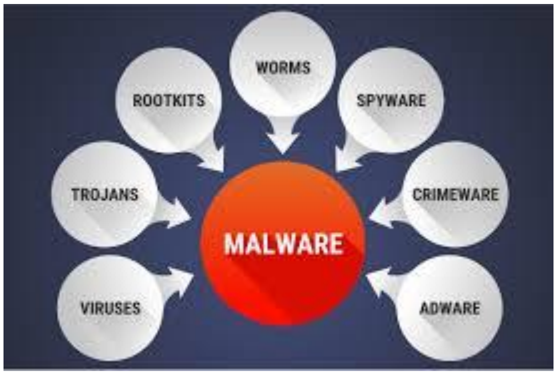

Figure 1: Types of malware from Crackart

4. **Social engineering and phishing:** Social engineering and phishing attacks pose major cybersecurity risks to schools. Students, teachers, or staff members who get manipulated to click on malicious links can provide cybercriminals access to the school's network and precious resources. The best way to counter social engineering and phishing attacks is through user awareness and training. Educating and testing your users with simulated attacks helps you facilitate a positive security awareness culture and makes them less likely to fall for scams. Make sure your email security is up to date as well, and that you have advanced protection for all your endpoints so you can protect them against both known and unknown malware, ransomware,

exploits, and viruses.

Figure 2: Phishing from Malware Bytes

5. **Mobile security:** Mobile devices like phones, tablets, and others are increasingly used today for remote learning. A single unprotected device increases the risk of compromising the entire school network and systems, especially at a time when schools have lowered the barriers to access their networks, specifically for students. With most devices connected to the internet, the attack surface is significantly amplified for schools. An effective mobile device security solution can help keep your students and staff safe on the internet, preventing risky file downloads and blocking access to inappropriate websites. Mobile antivirus and ransomware protection capabilities can safeguard your users and devices from malicious content and apps.

Common security mistakes in emerging educational technologies

Even though there is greater awareness of the threats education institutions face, the attack frequency on such institutions continues to increase. So, what are schools doing wrong?

1. **Weak security controls**: Schools today use a lot of emerging education technologies, including mobile learning apps to cloud-based tools. Depending on the size of the school, the number of security controls necessary can become overwhelming and result in poor or negligent implementation. Many times, schools add new technology but fail to expand their security protocols as well.

Figure 3: Online Impersonation from Cyber Bullying is Evil

2. **Limited IT personnel**: Budget allocations are coveted at schools. Every department wants more resources, which can lead to reduced funding for the IT department. Without the proper staffing to monitor networks and devices, having security controls will only go so far in protecting personal and academic information.

3. **Human Error**: If you have ever attended a school, you know that the admissions department and recruitment offices tend to leave their doors open. The goal is to create a welcoming environment that draws in prospective students. However, from a security perspective, such practices make information vulnerable. Other common mistakes that plague every industry include leaving passwords on sticky notes and clicking on malicious links and emails.