Back to School – Keep Students and Teachers Safe Online

PONDURANCE

The new school year is about to begin and with many schools investing in new technology, staying safe online has even more importance this year. K-12 ransomware attacks increased in number and severity over the past year accounting for 57% of all attacks, according to the FBI.[1] It's important for students and teachers to be prepared and know what to look for so they don't become victims of a cyberattack. Below are our top six tips for how students and teachers can stay safe online this year.

□ Keep software up to date.

Regularly updating software on your devices helps eliminate vulnerabilities that bad actors could use to launch a ransomware attack. Software developers are constantly looking for bugs and vulnerabilities in their software, and they release updates when patches are available. This makes it even more important to stay on top of software updates.

□ Install antivirus software.

Antivirus software allows you to block malware and other malicious software from infecting your system and your school's networks. It's best to have a solution that automatically updates and scans for viruses regularly. There are even some that incorporate antiphishing to add another layer of defense!

□ Use strong passwords.

You should choose strong passwords that are at least eight characters long and contain a combination of uppercase and lowercase letters, numbers, punctuation marks, and other special characters. Multifactor authentication is a great tool to use as well that requires users to provide two or more verification factors to access an account — either over email or through a mobile device.

□ Take security awareness training.

Cyberattacks are changing every day, making regular security awareness training even more important. Phishing and social engineering are on the rise making it important for end users to be able to detect when they are victims of one of these types of attacks.

□ Learn how to detect phishing emails.

Phishing emails are a common gateway for attackers to launch much larger attacks such as ransomware and malware. Through security awareness training, students and teachers will learn how to identify a phishing email and what to do if they receive one. When in doubt, DO NOT CLICK!

Learn more about security awareness training and how it can help in our blog ***Training to Prevent Phishing Attacks***.

Sources:

[1] K-12 ransomware attacks are increasing in severity – now is the time to get protected, Security Boulevard, Jun 2021.

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204