CYBER READINESS
INSTITUTE

Back-to-School: Keeping Educators and Students Safe

Educators, students, and parents across the world are in uncharted territory as cybercriminals begin to target the systems that support public and private educational institutions. Last year, 56% of K-12 schools report being hit by a cyber attack, according to an independent survey of 5,600 IT professionals in 31 countries.

As remote learning still remains an option for many students, and teachers are forced to grapple with new technologies and systems provided to enhance the student's learning experience, it's critical that everyone practice basic cyber hygiene.

Here are some easy steps that teachers, students, and parents can take to protect their online safety and security in the classroom and at home.

The Basics

Strong Authentication

- ✓ Ensure Multi-Factor Authentication is enabled on all systems and applications that support it.
- ✓ Develop strong passwords/passphrases that cannot easily guessed and does not include your address or personal names. We recommend at least 15 characters for a strong password!

Software Updates

- ✓ Make sure your operating systems and applications are set to automatically update.
- ✓ Accept all relevant software updates when offered basis. Do not delay!

Phishing

- ✓ The sad fact for anyone online is we can expect to see online scams, social engineering, and phishing attacks. Hackers and criminals are sure to use concerns about virus spread and the insatiable desire for news to trick people.
- ✓ Use consistent subject lines with students and parents so they can more easily validate that emails are from you.
- ✓ Always "mouse" or "hover" over the email sender's name to determine the sender's true origin.
- ✓ Pay close attention to a sender's name and email.

Secure Storage & Sharing

- ✓ Ask your school or district about its subscription to a cloud-based data storage provider so that you can access documents and share them in a secure way.
- ✓ Try not to use USBs. They are often infected with malware that can damage your computer.

Video and Chat Applications

- ✓ You may not have the option to choose the video platform you use because schools are engaging large contracts with vendors. When possible, ask for a secure, encrypted communications platform/app.
- ✓ Remind your students – and yourself – to block video and audio by turning off these functions when not in use. You can also block the video camera using a piece of heavy tape or a video slide.
- ✓ Make sure you know the person who is trying to video chat with you.

How to Make it Easy for Your Students

Teach your students the "ABCs" of good cyber hygiene:

A – Authenticate your accounts by using strong passphrases.

B – Beware of phishing attempts and help students verify that you are the sender of the email.

C – Caution students to only use their video app if they SEE your screen name calling.