CYBER READINESS
INSTITUTE

Keeping Educators and Students Safe

Our nation's educators and students are in uncharted territory as remote learning becomes the norm for school systems across the country. Remote learning brings tremendous opportunities that we could not have imagined 30-40 years ago.

For teachers, it means that their mission can continue. For students (and parents), it means the classroom has no boundaries and an adjusted sense of normalcy can exist in these uncertain times.

We are fortunate that today's advanced technologies will enable teachers and students to continue to work together. It also means we need to take precautions to ensure that we are all protected.

There are some easy steps that teachers can take to protect their online safety and security and that of their students.

The Basics

Passwords/Passphrases

Passwords/passphrases remain the best way to lock personal data and applications. Remote schooling also means that we all need to focus on securing our home networks.

- Ensure that your home router password/passphrase (passphrases are more secure than passwords) is not easily guessed and does not include your address or personal names.
- Enable multi-factor authentication (password/passphrase + one other requirement such as a text message) for access to critical data in cloud applications, which is important for data and document sharing with your students.

guide@cyberreadinessinstitute.com

Patches

Operating system security patches must be accepted and stay up to date.

- Make sure your operating systems are set to automatically update.
- Accept all relevant security patches on a weekly basis.

Phishing

- The more of us who are online over the coming weeks, the more we can expect an increase in 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 your students so they can more easily validate that emails are from you.
- Always “mouse” over the email sender’s name to determine the sender’s true origin.
- Remind your students to pay close attention to a sender’s name and email.

USB Use

With everyone working remotely, we are tempted to use USBs or removable media devices to transfer information – from a school computer to a home computer.

- Ask your school or district about its subscription to a cloud-based data storage provider so that you can access documents and share them with your students in a secure way.
- Don’t 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 in 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.