K-12 CAM 2020 VIDEO: Week 1 - Work Teach and Learn from Anywhere (Transcript)

Work, Teach and Learn from Anywhere

The world of education has changed significantly recently. Working from home, and teaching and learning in a remote or virtual learning environment have become the "new normal".

When you work in the office, or in your schools, you benefit from security measures that protect our networks, systems, devices, and information from cyber threats.

Moving from this trusted environment to remote work locations can increase security risks.

In this video, you will learn how you can help keep your board's and your students' information secure while working from anywhere.

The first source of risk we are going to examine is your devices.

When assigned a board-owned device you should never share it with anyone else. You should keep it secure, and you should follow the guidance provided by your board regarding the acceptable use of the device.

If you are using a personal device, no private or confidential information should be stored on that device.

You should not forward information from your work accounts to your personal device. If using a private device any work should be conducted 'in the secure cloud' and saved there. Examples include: D2L/Brightspace, Google Apps For Education, Microsoft O365 and other board provided cloud-based applications.

By accessing these applications through a browser and not downloading information to your personally-owned device you are keeping the information secure.

If you do use a personal device you should ensure that you have up to date anti-virus/ anti-malware installed, and that the operating system is up to date.

If the device is shared, have separate log in accounts for all people that share it, and ensure that when you are finished work, you close all browsers and log out of any cloud accounts.

If your board-issued device is lost or stolen, report the loss immediately to your principal or manager, and your board's IT Help/ Service desk.

The second source of risk we will examine is your home network.

Your home Wi-Fi network is critical to making your workspace cyber secure.

One of the easiest ways to increase your home cyber security is to change your Wi-Fi password from the default that comes with your router and to use a strong password that is difficult to guess.

Only use wifi networks that you know are secure, eg your board or your home wifi network. Be very wary of using external wifi networks such as in cafes, restaurants, hotels, etc for work purposes.

Cybercriminals can set up false networks that will record your activity, including your usernames and passwords. These networks look very similar to commonly found public wifi networks.

A good tip here is to use your cellphone as a hotspot if you are in any way concerned about the validity of the network.

The final source of risk we are going to examine are phishing emails.

Phishing email messages often try to create an impression of urgency in order to scare you into clicking on a link or divulging information.

You should always be suspicious of any email asking you to update your passwords and login credentials.

If you suspect an email sent to your board account is a scam, report it to your local IT department immediately.

If you have clicked on a link and/or filled in your credentials, please do not be embarrassed, it is critical that you report this information immediately to safeguard your account and prevent more widespread disruption.

If you receive an e-mail that you think is a scam to your personal account, use the same critical techniques to analyze whether it might be a scam.

If in doubt do not click on any links and contact the institution directly through secure means.

If you do click on a link and enter your details, immediately change your password on that account and any others on which you may have used the same password.

Thanks for Watching