MAY 2020 VOL. 7.B

CYBER MONDAY

A monthly cyber-security and data privacy bulletin from the UGDSB

Tips #1-3 were shared in Part 7A. of the May Cyber Monday bulletin. If you missed it please follow the UGShare link in the sidebar to view it.

Tip #4 - Use board-approved/evaluated devices and applications

A common method used by cyber-criminals to try to access and steal sensitive information is through pre-existing vulnerabilities – such as by circumventing weak or missing security measures on operating systems, applications or tools being used. If you have a board issued device for working remotely, you should only use this device for work-related activities. Only use board-approved/board-evaluated applications and web-based tools. Board approval of applications helps to ensure that the proper security measures are in place.

IN THIS ISSUE

SECURITY TIPS FOR WORKING REMOTELY

TIPS # 4-7 OF 11 TO STAY SAFE ONLINE

STAY TUNED FOR MORE TIPS NEXT MONDAY

CYBER MONDAY BULLETIN- MAY 2020 PART 7A.

CLICK HERE TO VIEW PDF

CLICK HERE TO VIEW ONLINE

Tip #5 - Limit access to the device you use for work

If you are using a board-issued device, only the approved user should use the device; family and friends should not use it. This minimizes the risk of the board-issued device being compromised. If you are using your own personal device for work, try to limit it to work-related use. If not possible, try to limit those who can use the device and ensure other users follow proper cyber hygiene practices such as only installing software from a trusted source and by following the tips from the Cyber Monday articles.

Tip #6 - Protect sensitive data and think before saving locally or printing at home

Be aware of privileges - access to sensitive data - that you may have while working remotely. You should avoid saving data and files locally when using your personal device for work purposes and avoid printing documents that contain sensitive or personally identifiable data. If printing is necessary, store paper records that include confidential or personal information in a locked cabinet or desk drawer when not in use and safely shred any paper records when no longer needed.

Tip #7- Secure your devices and keep software and apps up to date

Cyber-criminals scan for and look to exploit software vulnerabilities on internet-connected devices. To reduce this risk: Install endpoint protection (commonly referred to as anti-virus/ antimalware software) on your devices from a known and trusted source.Keep software and applications (e.g. operating system, anti-virus/antimalware, internet browser, and productivity applications) on your devices (PCs, smartphones, tablets) up-to-date at all times. Follow notifications to update software on your devices as these updates often address security vulnerabilities.