MAY 2020 VOL. 7.C

CYBER MONDAY

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

Tips #1-7 were shared in Parts 7A and 7B of the May Cyber Monday bulletins. If you missed either, please follow the UGShare links in the sidebar to view it.

Tip #8 - Secure your home network and avoid unsecured WiFi connections

Cyber-criminals may intercept personal or sensitive information by attacking unsecured Wi-Fi connections. To mitigate this risk you should ensure passwords on your home internet router and your home Wi-Fi network are strong and updated regularly and you should avoid using unsecured guest Wi-Fi networks (where no security key is required).

IN THIS ISSUE

SECURITY TIPS FOR WORKING REMOTELY

TIPS # 8-11 OF 11 TO STAY SAFE ONLINE

CYBER MONDAY BULLETIN- MAY 2020 PART 7A.

CLICK HERE TO VIEW PDF
CLICK HERE TO VIEW ONLINE

CYBER MONDAY BULLETIN- MAY 2020 PART 7B.

CLICK HERE TO VIEW PDF
CLICK HERE TO VIEW ONLINE

Tip #9 - Backup your data

Should your device be compromised by a virus/malware or be lost or stolen, having a backup of your data will allow you to recover or continue working from another device. When you back up your data, you create a copy of some or all files on your device and store them in a separate location (e.g. school network folder). Some backup software can also store your device configurations to provide a restore point for the device. Backup and recovery software can automate the process by performing backups on a set schedule.

Tip #10 - Take immediate action if a security incident is suspected

If you suspect your personal device or board-issued device may have been breached, immediately disconnect the device from your home network and power it down before taking further action.

For compromises on board-issued devices, or any suspected privacy violation follow the board's protocols and any reporting procedures that are in place.

Tip #11- Always adhere to board policies and procedures

Follow the guidelines and/or best practices as outlined in the Responsible Use of Digital Technology related to the use of IT systems, devices and resources. Staff should only use application software/systems that have been reviewed by the software vetting committee and approved for board use, as outlined on the Support For Green Tools webpages.

ADDITIONAL SECURITY RESOURCE LINKS:

useful resources from the Federal Government's Get Cyber Safe website (www.getcybersafe.gc.ca)

- Make yourself more cyber secure (in five simple steps!)
- Protect Your Devices
- Software updates: Why they matter for cyber security
- Signs of a phishing campaign: How to keep yourself safe
- The 7 Red Flags of Phishing
- Protect While You Connect — How to Stay Safe Online
- 5 ways to protect your privacy on a new smart device
- Here are three ways to keep mobile devices cyber secure
- Get Cyber Safe Blog
- The Canadian Anti-Fraud Centre