Cybersecurity Concerns

Potential Threats	Suggested Solutions
Scams/phishing	• Beware any remote desktop tools, phishing emails or unknown sites • Check sources/email addresses before opening messages • Beware sharing personal information or opening attachments
Unsecured (public) wifi network	• Avoid public wi-fi for teaching/official business • Use HTTPS sites • Read privacy agreements • Turn off sharing • Use a VPN
Using personal devices and networks	• Use strong passwords • Set up two-factor authentication • Use an antivirus software • Install updates regularly
Data loss	• Backup data regularly (cloud or external drive)
Hacking (by student or other)	• Use school email address for all school-related accounts • Create complex passwords and/or two-factor authentication • Change passwords often • Use different passwords for different accounts • *Use a password manager
Privacy	• Google yourself to check what private information is publicly available • Check privacy settings on social media accounts • Delete or deactivate old accounts
Cyberbullying	• Ensure live sessions are supervised at all times • Communicate/enforce guidelines for online behavior

Resources:

Shifting to Remote Learning

Teacher's Guide to Cybersecurity – Everything You Need to Know in 2020