Phishing Awareness during COVID-19 Pandemic

With the increased volume of communication coming from a number of sources on the coronavirus disease (COVID-19) pandemic event, you can expect an increase in the number of phishing attacks your organization will experience. These are email-based attacks through which cyber attackers try to entice email recipients to click a link or open an attached file in an attempt to trick them into providing personal, financial, or other sensitive information. If you open one of these links or files, it can infect your computer, and it can compromise school/division networks and systems—potentially resulting in major security breaches, reputational damage, and financial impacts.

Please remind all your employees and contractors to be vigilant at all times about email communications, whether at a school or school division facility/hub or at home. Ask them to follow these guidelines:

- Do not open emails from suspicious or unknown senders. If you are not sure, you should confirm with the purported sender or with your supervisor.
- Do not click on attachments or links from suspicious or unknown senders.
- Immediately report suspicious emails to your school and/or divisional IT department contact.