

Friday, May 6, 2022

The following is information sent to Near North District School Board (NNDSB) by the Ministry of Education, to be shared with our families:

With phishing scams on the rise, student and parents are asked to exercise heightened awareness to avoid being victims of cyber-crime.

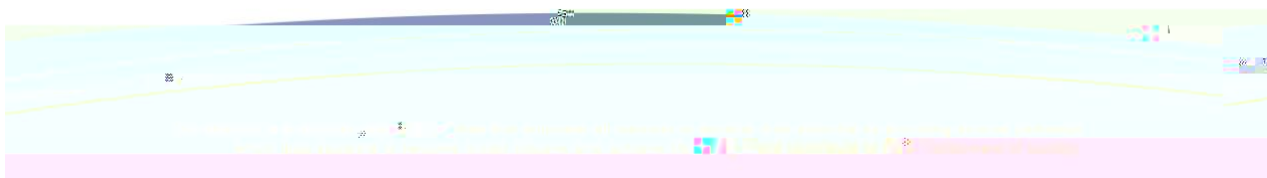
While most phishing attempts come by email, phishing can also come by other means. Phishing text messages (also known as SMS phishing or smishing) are fraudulent text messages, sent by cyber criminals, to try to lure victims into revealing personal or financial information to commit fraud or steal sensitive information or to click links that will install malware used to steal data and damage networks. These messages can arrive by SMS, iMessage, social media platforms, and other messaging platforms.

Phishing text / email messages are disguised to look like they are sent from a trustworthy organization or reputable person. Always use caution before responding to requests for information.

How it works:

Phishing scams typically use a threat or opportunity to encourage you to click a link or call a number. Financial incentives, including government payments and rebates, contests, prizes and giveaways are often part of the lure used by cyber criminals, as well as threats such as legal action, overdue payments or missed deliveries.

In the example below, the smishing screenshot is impersonating a Canada Revenue Agency payment. However, the cyber criminal is attempting to steal the information or infect the device of the user who clicks the link.



Tips to protect yourself:

Do not reply to the text message, do not call the number, do not click on any links in the message. Clicking a link could give cyber criminals access to your information.

Do a web search of the phone number and message. Chances are you are not the first person to receive this message.