Information on Phishing and Spam to help keep DDSB Families Cyber Safe

What is Phishing – Phishing is when someone is trying to get you to divulge personal and confidential data like your login ID and password, banking, or other privacy information by pretending to be a person or an organization that you trust. This is dangerous as the information can be used to access your important personal data.

What is Spam – Spam email is unsolicited and unwanted junk email sent out in bulk to indiscriminate recipient lists.

The common medium to deliver a phishing attack is by email. When you receive an email that looks suspicious, stop and "Think Before you Act". Below are some top things you can do to ensure your cyber safety:

Take a moment to analyze the situation

- Are you expecting the email? Be extra careful with emails which you are not expecting to receive. For example, a courier mail delivery notification by email or discount coupons.
- Does the link make sense? Don't click links or attachments that you aren't expecting.

Are you able to verify the sender? Don't provide any personal information unless you know that it is legitimate.

- Verify that it's legitimate by calling the sender for verification.
- Verify the hyperlink behind the link's text or button by hovering over the text.

How can I recognize that a message may not be genuine?

- Check the email address for suspicious spelling or language.
- Look for inconsistencies like pixelated logos or misspelling.
- Can you spot the difference in info@amazon.ca and info@amaz0n.ca? The second one has a spelling mistake and uses the number "0" in place of the letter "o".

The Government of Canada has a national public awareness campaign created to inform Canadian about cyber security and the simple steps they can take to protect themselves online. Visit getcybersafe.gc.ca/en for more information.

By working together, we can all stay cyber safe!

DDSB
Ignite Learning