Hey Everyone,

Cyber threats like phishing are on the rise. Here's how to **spot** and **avoid phishing emails**.

🎣 What is Phishing?

Phishing is when scammers send **fake emails** pretending to be trusted sources (like CLASS) to **steal personal information**.

🚩 How to Spot Phishing Emails

Emails being received from domains out of class's will be flagged with the message below **PLEASE BE ADVISED THAT THE SENDER OF THIS EMAIL IS FROM OUTSIDE THE CLASS ORGANIZATION!**

- **Public Domains**: CLASS emails come from **@class.on.ca**. Be cautious of free domains (like **@gmail.com**).
- **Misspelled Domains**: Check for **small typos** in the domain (e.g., **@cllass.on.ca**).
- **Poor Grammar**: Phishing emails often have **typos and awkward language**.
- **Suspicious Links or Attachments**: **Hover over links** to check before clicking.
- **Urgent Language**: Be wary of phrases like **"Immediate Action Required"**.

🧐 Suspicious Subject Lines

- **"Account compromised"**
- **"Payment required"**
- **"Password reset request"**
- **"Password Expires/Password has expired"**
- **Urgent Notices**

Pause and verify before clicking.

✅ What to Do

- **Don't click** links or open attachments until verified.
- **Check the sender's email address** for typos or errors.
- **Contact IT** if unsure: **itsupport@class.on.ca**.

Stay vigilant! 🛡️