

Cyber Scams and Phishing:

Don't be a victim!

A cyber scam is an online criminal activity designed to scam people out of money or personal information.

Most common types of online scams

- **Phishing, Vishing, and Smishing** is a technique to “fish” for usernames, passwords, and other sensitive information, from a “sea” of users – through emails or text messages.
 - Phishing emails, smishing text messages, and vishing audio/phone messages may look like they're from someone or a company you know or trust.
 - These messages urge you to click a link, open an attachment, call a number or contact an email address.
 - The victim is then tricked into providing their personal information and credentials to other websites or services.
- **Fake apps** are apps created by cybercriminals to cause harm to users and their devices. They are designed to look like real apps but instead monitor your activity, install malware, or steal your personal information.
- **Websites that sell fake products.** These sites offer cheap products that never arrive.
- **Formjacking** is when a legitimate retail website is hacked, and shopper information is stolen.

How to avoid scams:

- Do not open attachments, do not click links and do not respond to suspicious messages. Ask questions, consult people you trust, or contact the sender using an alternative communication method.
- Avoid suspicious apps and deny permissions for something the app shouldn't be doing.
- Always use secure sites (**look for the S in https://**) when shopping or logging into your accounts online.
- Buy products from known sites only.
- Do not post personal information on social media.

If you think you may be a victim of a scam:

- Stop all communication with the scammer.
- Seek help from an adult you trust.
- Report the scam to your teachers or parents/guardian.



**/DIGITAL
{ME}**

Funded by:



For more information: www.K-12CyberAwareON.ca

© King's Printer for Ontario, 2025