Resources and Reporting

Get informed: Consult the following documents and / or websites to learn more and access help, in the case of serious forms of cyberbullying or cyber scams.

- Provincial School Code of Conduct Policy
- Bullying & Cyberbullying: What We Need to Know, A Reference Guide for Parents and Guardians
- Nova Scotia Health: Mental Health & Addiction Services
- Kids Help Phone
  Phone: 1-800-668-6868 **Text**: 686868

Report: Inform the appropriate authorities, of serious forms of cyberbullying or cyber scams, which may include teachers, principals and police personnel.

Nova Scotia CyberScan Unit
Phone: 1-855-702-8234

Online Reporting Form: Bullying / Cyberbullying, for Students, Parents and Guardians

RCMP·GRC Royal Canadian Mounted Police

Strait Regional Centre for Education — Contact your local school.

Be a Part of the Solution

Stand up for human rights by refusing to forward text messages or photos that are hurtful, demeaning, or disrespectful. The resources above will help.

Social Media

Be Kind

Treat others as you would like to be treated. Remember you are interacting with real people on forums, comment sections, digital and social media platforms.

Don't feed the trolls. Any response will only encourage more negative comments. Do not engage trolls.

Don't take material that doesn't belong to you. Though it may be easy to use others work, remember you need permission and / or need to acknowledge work that is not yours.

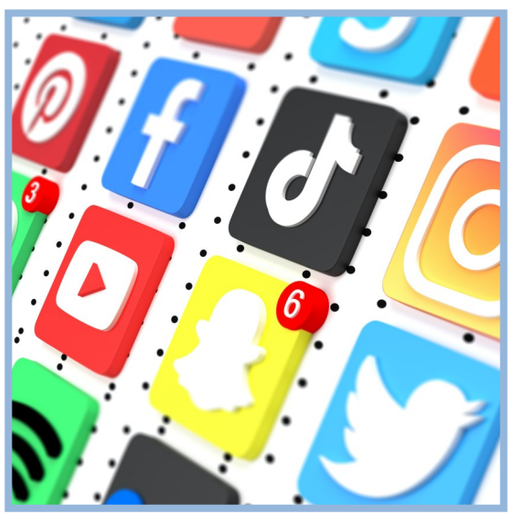
Don't believe everything you read online. Always take the time to investigate claims and confirm their validity and reliability. You don't want to be responsible for furthering misinformation.

Source: GCFLearn.org (2019) Being a Good Digital Citizen. Retrieved from https://www.youtube.com/watch?v=ju9aOc2MLyo.

Digital Citizenship

A Quick Reference Guide

Strait Regional Centre for Education



Strait Regional Centre for Education
304 Pitt Street, Unit 2
Port Hawkesbury, NS B9A 2T9
902-625-2191 / 1-800-650-4448
902-625-2281 (fax)
srce@srce.ca / www.srce.ca
X (Formerly Twitter) @SRCE_NS

Introduction and Definitions

Phishing is when a person attempts to obtain confidential information from an individual by pretending to be a well-known brand or someone of importance. Financial gain is usually the motive.

Types of Phishing

Smishing is done through a text message. Usually a link will be included within the message.

Spearphishing is designed to sound like a source you know personally. The message will appear to come from a credible source and contain relevant subject matter.

Whaling usually focuses on a high profile target (CEO of a company). These types of attacks are highly sophisticated.

Spoofing is a fake website created to trick someone into sharing personal information or entice you to download malware. For example, a website designed to look like a trusted banking institution or online store.

Know the Signs

Check the email address. If it ends with another domain or has a letter missing or added, it is likely suspicious.

Check characters carefully. For example, the lowercase letter A may be replaced with the letter α from a different alphabet.

Check for spelling / grammar errors. Text messages, emails, or websites with these types of mistakes, are good indicators of a phishing attempt.

When Unsure, Verify. Confirm the identity and contact information of the person by referring to an official source.

Stay Safe Online

Protect your reputation. Be yourself but be cautious. A post that at first seems harmless can easily be taken out of context, get distorted and go viral.

Be careful who you trust. Don't respond to open emails or accept friend requests from people you don't know.

Think before you click. Once something is online – a picture, a comment – it's no longer under your control.

Don't leave a trail. The information you include in your posts can be more revealing than you think. Depending on what you say, it can be easy for someone to figure out where you live, how old you are, and build a picture of your routine.

Stay anonymous. Use your real name for official accounts – for work and school – but if you're gaming online, use caution to protect your personal information.

Recognize the signs. Familiarize yourself with the most common cyber threats, for example, Phishing.

Keep your private information private. Change your privacy settings to the most secure and limit the type of information you share.

Source(s):

Office of the Privacy Commissioner (2021) Back to school tips for playing it safe online. Retrieved from https://www.priv.gc.ca/en/blog/20210902/.

Government of Canada (2023). Get Cyber Safe. Retrieved from https://www.getcybersafe.gc.ca/en.

Passwords and Privacy Settings

Choose a Secure Password

- Avoid pet's name or family member's birthday.
- Create a passphrase; a combination of four or more random words, with a minimum of 15 characters.
- Use at least twelve characters with a combination of upper/lowercase letters, numbers and special characters (e.g., @,!,$).
- Avoid using the same password for multiple accounts.
- Use a password manager to help remember them all.
- **NEVER** share your password with anyone.

Adjust Your Privacy Settings

Enable Multi-Factor Authentication (MFA) in your settings to keep your account secure. An additional verification, like a PIN, is emailed or texted to your phone.

Review Your Privacy Settings. Adjust your default settings to increase the security and privacy of your posts. Default settings typically allow access to your account.

Informative pictures can provide unique details to viewers. Check picture backgrounds before posting, look for revealing information like street signs or license plates.

Geotagged photos provide exact details of where a photo was taken. Turn off geotagging in your camera's settings and remove geotags from older photos with photo editing software.

Exciting news such as vacations, big purchases or events with your address inform scammers of times when you may be most vulnerable. Avoid sharing this information.

Banking or financial information including the name of your bank, credit or debit card numbers should never be made public at any time.