



**Grades
7-12**

Safety Online: Understanding Online Risks



**ROGERS
cybersecure
catalyst**



The Internet is a place where you can learn, connect with friends or family, play games, or stream your favourite shows or music. You can access it anywhere, any time, on any device – whether it's your phone, tablet or laptop. However, the Internet and the devices you use to access it come with risks; and without the proper awareness, you could fall prey to a variety of online dangers.

Teens, in particular, are frequently targeted because you don't yet have a credit history; this makes it easier for cyber criminals to assume your identity and open credit cards in your name. Be aware, and take care of your online safety and security.

This resource offers information on safety awareness, to empower you with the skills you need to understand the risks to both yourself, and your devices, when online – so you don't fall victim to scams or identity theft, or find your devices infected with viruses or other malware.



A DEFINITION

Online risks appear as scams, identity theft, and malware or viruses while using connected devices. In order to keep your private information and accounts safe, you also need to keep your devices safe. Check out the definition bubbles for descriptions of common terms and issues to look out for.



Scam:

Scammers, or people who participate in dishonest schemes and trickery, entice you to download or buy something, ask you to do quizzes, or offer things like money, prizes, gaming systems or free tablets.

Identity Theft:

Cyber criminals learn as much as they can about your private or personal information and use it to pretend to be you, to open bank accounts in your name. Scammers can also take over your gaming accounts and social media profiles.



A DEFINITION



Viruses:

Code designed to secretly copy itself onto computer files or programs to destroy data, and disrupt the functionality of computers and networks.

Malware:

A virus secretly installed with the intent to steal your private information, spy on your device, or encrypt your device until you pay money to the perpetrator.





B RELEVANCE

Avoiding online risks

These risks can come from virtually anywhere: browser add-ons and extensions, emails, text or direct messages, clicking on infected links, social media posts, chat rooms, ads or apps, and online gaming platforms – you name it.

New schemes are becoming increasingly sophisticated, and you can unknowingly give up confidential information that allows cyber criminals to access your accounts or create new ones in your name.

When you sign up for a new game or account, you need an email address. Unfortunately, scammers most commonly use email and text messages to send communications with the intentions to trick people. This type of communication is called spam.

Scammers:

People who send spam, or participate in lies by tricking people into giving them something, such as information or money.

Spam:

Unwanted or uninvited communication, most commonly in the form of email or text messages.

Phishing:

(Pronounced “fishing”) Fraudulent attempt or a scam by an Internet user to get private or personal information to use illegally.

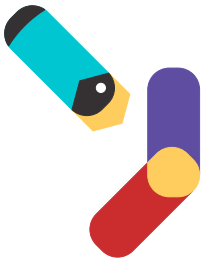
Spoofing:

When communication is disguised as being from a known source, like someone you know, when in fact it's from an unknown source, such as a scammer.

Preventing online risks

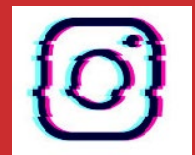
Follow the recommended steps below to help you avoid risks to devices and to yourself. These tips are specifically for email; however, a lot of these rules can apply to other forms of communication!

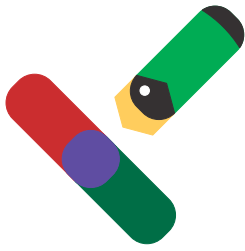
- **Do not reply to spam**, so the scammer won't know your account is active!
- **Do not click on any links**; instead hover your mouse over the link to see the real website. If the message states that your account has been locked, open your web browser and log into your account directly from the organization website to see if there's actually an issue with your account.
- **Do not click on or download attachments!** Contact the sender directly to learn more about any unexpected attachment before opening it.
- **Check the sender's email:** Hover your mouse over the email address or sender's name; if the email is from a friend, verify that it's the email address you have for that person. When in doubt, check it out! Contact the sender personally to see if the email was really sent by them.



Remember this:

If the email is something like **customerservice@instagram.cz** then chances are the email has been spoofed, as any email from Instagram would be **Instagram.com**





Preventing online risks

Follow the recommended steps below to help you avoid risks to devices and to yourself. These tips are specifically for email; however, a lot of these rules can apply to other forms of communication!

- **Check the subject line:** If you receive an email from a friend or family member and the subject line has a sense of urgency, such as "I need your help", call the friend or family member directly. If you receive an email from a company and the subject line reads "Your account has been suspended", tell a parent/ guardian and have them investigate it.
- **Scan for spelling and grammar mistakes:** If you receive an email from a real company, typically, there would be no spelling or grammar mistakes.
- **Beware of requests for personal information:** Kids should never share any personal information, including usernames, passcodes, account numbers, etc.
- **Junk/spam folder:** Train your email to automatically send spam to your junk folder, by moving it there each time you receive it. moving it there each time they receive it.
- **Block the sender:** This way, you don't repeatedly receive emails from them.
- **Delete the fake email:** Don't keep it in your inbox in case you, or someone else, clicks on the fake email.

Did you know?

You can join the fight against spam by reporting all spam emails to:
spam@fightspam.gc.ca



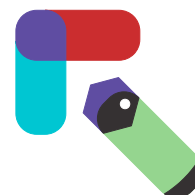
C CALL TO ACTION

Socializing safely online

Socializing with friends on gaming or social media sites is a fun way to connect with others. Unfortunately, cyber criminals can take control of your existing profile or create a new one in your name. They do this to send fake messages to your friends and followers, encouraging them to send money, or install malware in their devices – all while pretending to be you.

To protect yourself, your information and your devices, refer to this checklist:

- **When online, kids should only play games, chat, and follow or add friends that they know in real life!** It's easy to be flattered or curious about someone who's popular or has a lot of influence, but it's important to delete friend requests from people they don't know personally.
- **Don't be tempted by websites or advertisements that include a prompt to link their accounts or click on external links, quizzes or contests,** such as "find out who's talking about you" or "who has a crush on you" or messages telling you to click on links because "there's something you should see!"
- **Be especially careful with any links or attachments** on game chats and social media platforms, even if shared by friends. If they're not 100% sure, give the friend a call or send them a text message first!





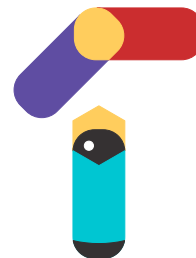
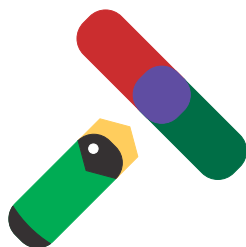
C CALL TO ACTION

Clickjacking

An ill-natured method of tricking someone into clicking on something different from what the user perceives, potentially revealing confidential information or allowing others to take control of their computer.

Socializing safely online

- **Be especially careful with any links or attachments** on game chats and social platforms, even if shared by your friends. If you're not 100% sure, give them a call or send them a text message first!
- **Only click or open posts from people you know in real life or reputable accounts.** Simply liking, sharing or unknowingly clicking on content posted on a hacked social media post can direct you to spam, malware or have malicious posts automatically show up on your profile. This is known as clickjacking.
- **Be aware of what you share!** Never share anything personal or private when socializing, even on a private account, as you may not know if a friend's account has been hacked and the hacker is accessing your information.



Browsing securely online

Visiting websites can open up a world of fun and exploration, but it can also expose you to a lot of unexpected risks. To protect yourself, follow these simple steps:

- **Block all pop-up ads and banners:** These distracting annoyances appear on websites, games, videos, etc., and you can block them by updating your settings on whichever Internet browser you use (e.g., Internet Explorer, Google Chrome, Firefox, etc.). This helps you to avoid accidentally clicking on them. You can also install ad blockers – just be sure to do your research first before installing them!
- **Browse websites that begin with https or a padlock:** These websites are the most secure – but, alone, do not guarantee protection!



- **Bookmark** websites that you visit frequently..
- **Use safe search mode** on your browser.
- **Periodically delete cookies** stored on your browser.

Cookies:

Internet cookies are built specifically for web browsers to track, personalize and save information about each user's session. A "session" just refers to the time you spend on a site.

Fraudsters have become quite sophisticated at spoofing or impersonating real websites. These fake sites mirror real ones so closely that it can be difficult to tell which is which. Unsure? Remember to:

- **Double check the website address:** These Scammers can make a website appear to be a real one by simply changing one letter (e.g., "o" to a "zero") or having a different ending of the web address (e.g., ".com" to a ".net").
- **Check the website's certificate:** Make sure the website you're visiting is valid by clicking on the padlock symbol in the address bar of your browser, and verifying that the website certificate is valid.



CALL TO ACTION

Downloading safely

There's so much to download, and a lot of it is free. This may seem exciting, but remember that not all that is free, is safe. Aside from copyright issues and the chance of the content being acquired illegally, the free games, wallpaper, ringtones, movies or music you download could be secretly bundled with malware and viruses. To protect yourself and your devices when downloading, be sure to:

- **Download only from trusted or reputable sites.** Always check the website address first! If you're not sure, look for your content on a more secure site. If you find that your download isn't available anywhere else, that may be a red flag
- Take the time to **carefully check the download link.** Check by hovering over the link to reveal the web address.
- **You may be tricked into downloading installers or plug-ins** in addition to the program you were seeking. Usually, you don't need any other program to download anything, so research the download carefully before proceeding.
- **Before downloading, back up your device.** Have your virus or malware scanner scan the program before downloading. Scan again after downloading, just to be sure.



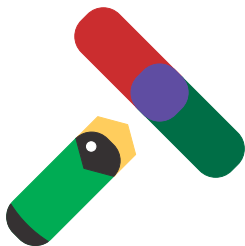
Did you know?

HTTPS at the beginning of a website address stands for Hypertext Transfer Protocol Secure – this is a very technical way of saying that there's secure communication over a computer network.

C CALL TO ACTION



Even if you're well-informed, and have all the latest security software, you can't let your guard down! Just like in real life, you could have all the home security to protect you – the best locks, floodlights, cameras, guard dogs, armed security guards and gates – but if you trust a delivery person to enter through the gates to come to your door without checking first, then you can be exposing yourself to risk. Recognizing and avoiding these risks will help you, and others, be safe online.



Reflect on your understanding:

What are some of the scams you've heard about? What are the best ways to protect yourself from these scams?

Tip!

If you accidentally download a virus or malware, disconnect your device from the Internet, and turn it off immediately. Take your device to a professional technician to solve the issue.

Activities are a useful way for you to test and demonstrate your knowledge on the topic covered in this resource.

Spot the Spoof!

Take a look at the sample email below.
Can you spot all the signs that this email is a spoof?



SPOOFS:

- 1) _____
- 2) _____
- 3) _____
- 4) _____

ANSWER KEY

1) "Hi Dear": This is a very casual/general/generic greeting; a reputable corporation like Netflix would typically address a customer by name!

2) <UPDATE ACCOUNT NOW>: Corporations commonly direct you to login to your account from a new tab or browser, not directly from an email link.

3) Visit here or contact us here: Corporations would suggest you go directly to their webpage, or give you their customer support email address or phone number to connect with.

4) "From your friends at Netflix": Not a typical sign-off, it's almost too casual!

Tricky Situations

Think about the situations below, using your new knowledge about device security. What do you do next?

1. You get an email alerting you that your account has been suspended. Do you...?

1

- a. Ignore it
- b. Click the link in the email
- c. Go to a web browser and sign into your account directly to see if it's true
- d. None of the above

2. You download a new app on your tablet and download a virus by accident. Do you...?

2

- a. Disconnect from the Internet immediately
- b. Shut down your device and bring it to a professional technician
- c. Ignore the problem and it will go away
- d. Both A & B

3. You get a direct message (DM) from a secret admirer with a link to their favourite music video. Do you...?

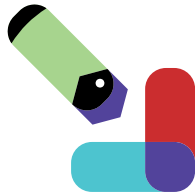
3

- a. Forward it to your friends
- b. Delete it
- c. Open it and click on the link
- d. All of the above

[answers] 1. C 2. D 3. B



FOR MORE INFORMATION



For more information on cybersecurity, or to continue the conversation and learning process, visit the Canadian Centre for Cyber Security website:

<https://www.cyber.gc.ca/en/>

Kids Help Phone:

Contact by text message at 686868 or by phone at 1-800-668-6868 from across Canada, 24 hours a day, 7 days a week; or access their resources online:
<https://kidshelpphone.ca/>



