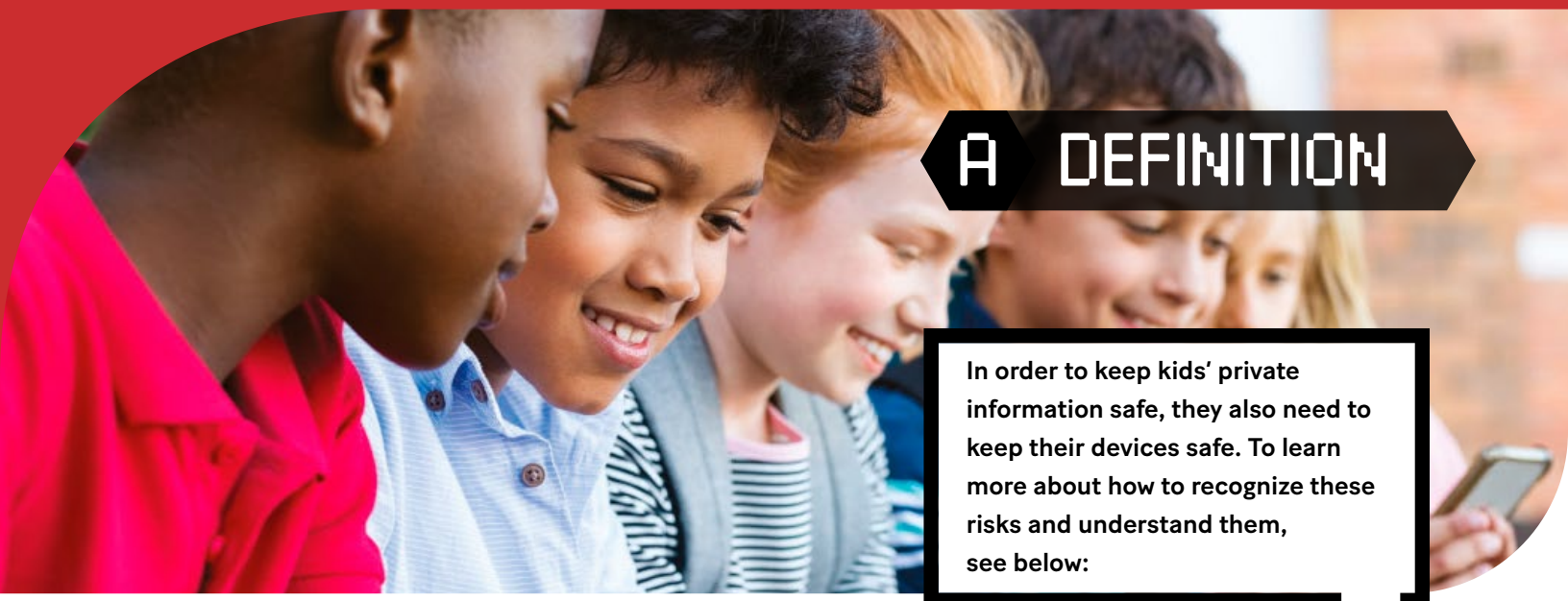
Grades 4-6

# Safety Online: Understanding Online Risks

ROGERS cybersecure catalyst

The Internet is a place where kids can learn; connect with friends or family via messaging, email or social media; play games; or stream their favourite shows or music. Kids can access the Internet virtually anywhere, and at any time, on any device – including phones, tablets or computers. However, using devices connected to the Internet comes with risks; and without the proper awareness, both kids and their devices could fall prey to some of the numerous online threats such as scams or identity theft, or have their devices infected with viruses and other malware.

This resource off ers information and guidance for parents/guardians to communicate with kids on how to spot potential risks while using devices connected to the Internet, and how to socialize, browse and download safely and securely.



# A DEFINITION

In order to keep kids' private information safe, they also need to keep their devices safe. To learn more about how to recognize these risks and understand them, see below:

## Scams

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


## Identity theft

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

## Virus

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

## Malware

- A type of virus secretly installed with the intent to steal kids' private information, spy on their device, or encrypt their device until they pay the perpetrator money.

# B RELEVANCE

## Avoiding online risks

- It's important for kids to be aware of the messages they're receiving on their devices, the real identity of the sender, and the actions they're being asked to take.

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

- Spam messages are often sent out by scammers, who use email or direct messages on social media – or, if kids have a cellphone already, through text messages – in order to trick people into clicking dangerous links. Scammers can also attach viruses to their messages to infect devices and accounts, preventing kids from using them further.

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

- The messages look so real, and can trick kids into giving up personal and private information, allowing scammers to gain control over their accounts. This type of scam is called phishing (pronounced "fishing").

**Phishing:** (Pronounced "fishing") Fraudulent attempt or a scam by an Internet user to get private or personal information to use illegally.

Ask kids to imagine being at a playground and a stranger offers them a free tablet... all they have to do is provide their name, address and phone number. Would they provide these details? Probably not! The same should be true for online scenarios like contests, advertisements or emails that seem too good to be true.

## Remember this:

B RELEVANCE

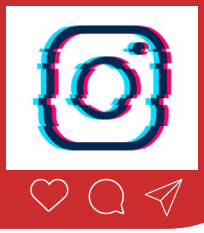
# Preventing online risks

**Review this list of tips with kids to help them avoid risks to devices, and themselves. 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 the kid's account is active!
- Do not click on any links: Have kids try hovering the mouse or cursor over the link to see the website address it's linking to. If the message is specifically about an issue with an account, such as Fortnite or TikTok, kids should open the web browser or app and log into their account directly from there to check it out
- Do not click on or download attachments! Kids should contact the sender directly and ask them if it was actually them who sent it. Better safe than sorry!
- Check the sender's email: If the email is from a friend or family member, or is schoolrelated, kids should verify that it's coming from the email address they already have for that person.
- Check the subject line: If kids receive an email from someone they know and the subject line seems urgent, like "I need your help", they should call or text them directly!
- Scan for spelling and grammar mistakes: If kids 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: Kids can train email to automatically send spam to the junk folder, by moving it there each time they receive it.

## 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 from Instagram.com



## C CALL TO ACTION

**Did you know?**

If kids come across these types of emails, parents/guardians can join the fight against spam by reporting all spam emails to:

**spam@fightspam.gc.ca**

# Socializing safely online

- There are many ways kids may use devices to socialize online: playing games virtually with their friends, or sharing pictures of their pets on social media. Scammers often use similar tricks mentioned above; they pretend to be someone else, and send friend, follow or message requests.

### To protect kids on these platforms, ask them to refer to this checklist when socializing online:

- **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 kids to click on links to see something super cool.**
- **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!**
- **Check the sender's email: If the email is from a friend or family member, or is school-related, kids should verify that it's coming from the email address they already have for that person.**
- **Kids should only click on or open posts from people they know in real life or accounts that are wellrecognized. Simply liking, sharing or unknowingly clicking on content posted on a hacked social media post can direct kids to spam, malware or have malicious posts automatically show up on their profile.**
- **Kids need to be aware of what they share! Never share anything personal or private when socializing, even on a private account, as kids may not know if a friend's account has been hacked and the hacker is accessing their information.**

# Browsing securely online

- How can kids keep themselves safe when browsing websites, watching videos or playing a favourite game they just downloaded? Scammers have many tricky ways to get people to click on something that may contain a virus, malware or spyware.

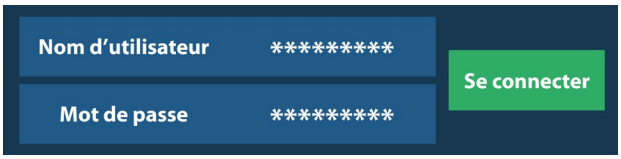
- Ensure kids are on the lookout for:


- **Pop-ups and banners:** Not only are these distracting, but they may contain viruses, malware or spyware. They appear on websites, games and even while watching videos! Kids need to be careful with their clicks to avoid nasty tricks.


- **Offers:** There are many promises of gifts, money or rewards. Nothing is truly free. There may be a hidden cost that they might not like, such as installing a virus on their device.

- **Online quizzes and contests:** Although it may seem very tempting to figure out which ice cream flavour they are or which Pokémon character they most resemble, these nosy scams are only looking to collect kids' personal and private information, either by requiring them to fill out information before beginning, or by linking to one of their online profiles.

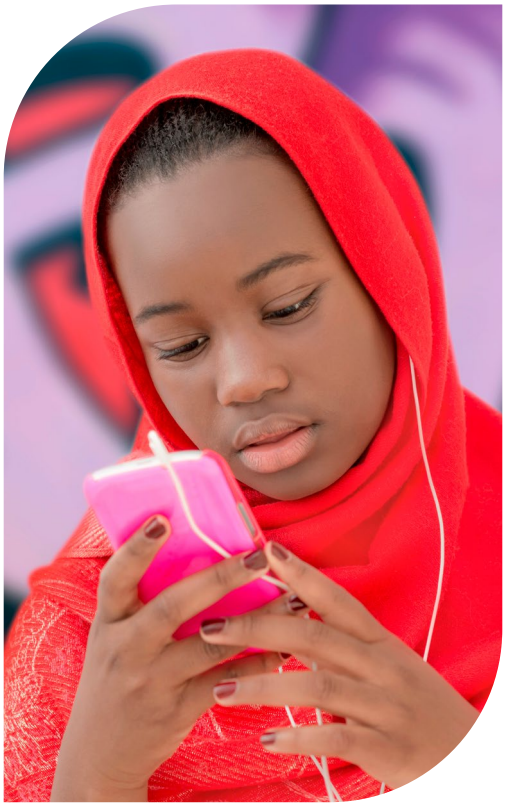
- **Auto-fill:** Do not allow Internet browsers, such as Firefox or Safari, to auto-fill (or store) kids' data, such as first name, last name, date of birth, address, etc., as it can potentially be distributed to other people or companies unknowingly.




- **Fake websites:** Scammers can create fake websites, especially websites that look a lot like the real version; and hope people don't notice, and then enter personal and private information, or accidentally install a virus on their device. Stick to trusted website. Once kids find a trusted website, if they think they may visit it often, ask them to take the extra step to bookmark it for future use.

# CALL TO ACTION

## Downloading safely



- There's so much to download from the Internet, and kids may not even realize that what they're doing is considered "downloading". Anytime they want to save something to their computer, tablet or phone, they usually have to download it first; this could include new or updated mobile apps, photos and videos they want to save for later, or electronic documents.
- A lot of what they download is free, and this may seem exciting – but, remember, not all that is free, is safe. Free games, wallpaper, ringtones, movies or music could secretly be infested with malware and other viruses.

**Conversation Starter:** Have you ever come across spam emails or messages before? What did you do with them? What are scammers trying to gain by sending these types of messages?


## Tip!

**Not sure how to determine if a website is safe to download from? Look for the HTTPS and the padlock symbol in the address bar! HTTPS:// at the beginning of a website address means there's a secure communication over a computer network**

# CALL TO ACTION

## Preventing online risks

**To protect kids and their devices when downloading, ensure they:**

- **Download only from trusted or reputable sites. Kids should always check the website address first! Remember to look for the "HTTPS" and the padlock symbol in the address bar.**


- **Take the time to carefully check the download link Kids need to remember to hover the mouse or cursor over the link to reveal the web address before clicking – do they match? Do they have odd or extremely long website addresses?**

- **As a precaution, it's best practice for kids to back up their device before downloading; this could mean saving important files to an external hard drive, or backing up a phone to a computer.**

- **Parents/guardians should educate themselves on the latest scams and news regarding device safety. If kids accidentally download a virus or malware, make sure they disconnect their device from the Internet, and turn it off immediately. Take the device to a professional technician to solve the issue!**

This resource has provided important information to share with kids, to make them aware of potential online risks, and how to prevent themselves from being tricked into sharing personal or private information. If kids ever find themselves in an unfortunate situation, they should tell a trusted adult immediately. The longer they wait, the worse it could get.

# ACTIVITY 1

Activities are a useful way for kids to test and demonstrate their knowledge on the topic covered in this resource. Have them try the activities themselves, and offer support when needed.

## Safety Online: Understanding Online Risks Word Search

Can you find the keywords related to understanding and avoiding online risks? As you find the words listed below, think about what they mean, what you've learned, and how you can help share this information with others!


Communicate

Attachments

Message

Sender

Trick

Fake

~~Safe~~

Spam

Beware

Personal

Delete

Email

**Remember this:**

**Trust your gut.**

**If it looks suspicious, steer clear!**

ACTIVITY 2

# Spotting Fake Websites

**Below are two versions of popular websites: one is the correct website address and one is a fake. Can you tell which website is the correct one, and how do you know?**

**Khan Academy:**
**A non-profit educational organization created with the goal of creating a set of online tools that help educate students**

1

**a.** https://fr.khancademy.org/

**b.** https://fr.khanacademy.org/

**Kahoot!:**
**A game-based learning platform, used as educational technology in schools**

2

**a.** https://kahoot.com/fr

**b.** https://kah0ot.com/fr

**Safe Search Kids:**
**A friendly Search Engine for Kids powered by Google**

3

**a.** https://www.safesearchkids.com/

**b.** https://www.safesearchkids.cz/

[answers] 1. B - answer A is missing an "a" in academy 2. A - answer B has the number "0" instead of an O
3. A - answer B ends in .cz instead of .com or .ca

# 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/

Toronto Metropolitan University

ROGERS cybersecure catalyst