Grades K-3

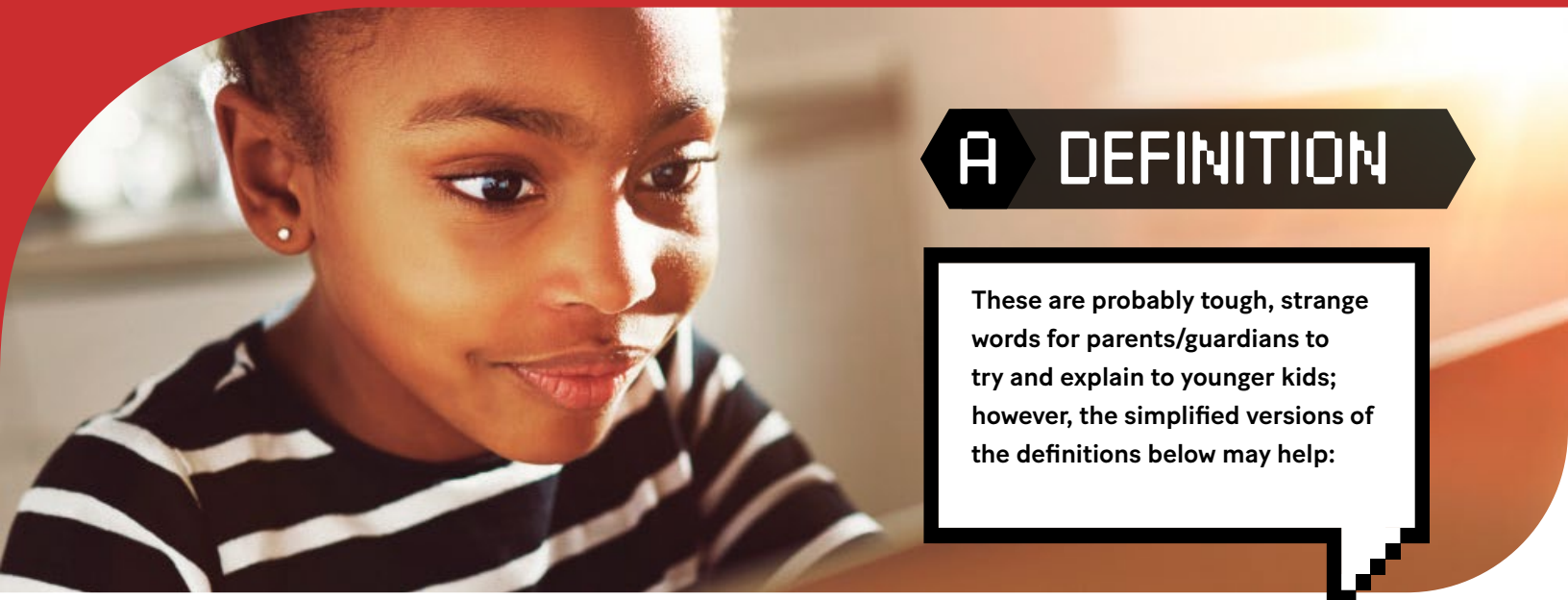
Safety Online: Understanding Online Risks

ROGERS cybersecure catalyst

Younger kids can think of the Internet as the entrance to a big playground in the online world! They should be closely monitored when using devices connected to the Internet, including laptops, computers, tablets, cellphones, gaming systems, smart TVs and more.

If parents/guardians are letting kids explore this 'online playground', it is imperative that they discuss the many possible risks – to both the kids and their devices.

This resource offers information and guidance for parents/guardians to communicate with kids about the potential risks while using devices, and how to spot and avoid these risks while socializing, browsing and downloading online.



A DEFINITION

These are probably tough, strange words for parents/guardians to try and explain to younger kids; however, the simplified versions of the definitions below may help:

Scams - Risk Definition

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

Scams - Risk Explanation for Youth

- Sometimes there are bad people who use the Internet to send messages on devices to try and trick kids into giving information like their name, age or address. Kids should always ask an adult first before clicking on pictures or links, or opening messages from unknown people.

Virus - Risk Defi nition

- 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.

Virus - Risk Explanation for Youth

- Think of a real-life virus, like a cold or the fl u, but instead it's for a device. If kids' devices, like tablets or phones, get sick, they stop working properly.

A DEFINITION

Identity theft - Risk Definition

- 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.

Identity theft - Risk Explanation for Youth

- Sometimes there are bad people who try to use information about kids, including their pictures, names or favourite things, to pretend to be them. These bad people do this to try and trick other people into helping them. This is why kids should never post any private information online without telling an adult first!

Malware - Risk Definition

- 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.

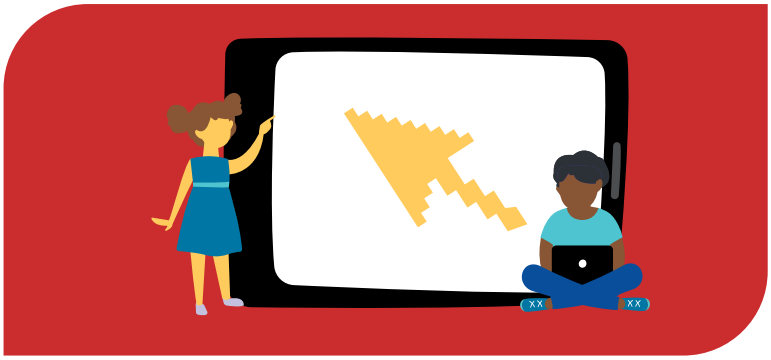
Malware -Risk Explanation for Youth

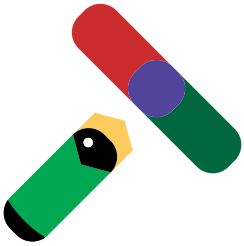
- A type of virus that can be on a computer or other devices, without anyone knowing. It is silently stealing information from the devices, like passwords, pictures, and possibly deleting files that they might need later!

A DEFINITION

Avoiding online risks

- All these risks can come from various forms of communication and interaction with devices, including emails; text messages; chat functions available in virtual worlds or online games; infected links to websites; or downloadable banner ads, pop-ups on websites, social media posts and apps.





B RELEVANCE

- 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.

- Scammers, or "bad people", try to take advantage of kids' innocence and lack of experience using devices connected to the Internet, to try and trick them into giving up personal and private information. This is called phishing (pronounced "fi shing").

Remember this:

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.

B RELEVANCE

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

- **Do not click on any links, photos or videos, pop-ups or advertisements that kids are unsure of, or visit new websites or download games without asking a parent/ guardian first!**

- **Tell a trusted adult whenever they are using a device and they receive any sort of message. Kids should be sure to not share or forward any messages that they're unsure of – if they contain viruses, they may put others at risk!**

- **Do not reply to messages or accept friend requests from strangers online. This means not answering or replying to phone calls or text messages from unknown people or numbers.**

- **Think before clicking! If something seems weird, or too good to be true, like someone offering a free toy or prize for doing a quiz or filling out a form, don't go for it. Kids should never share any sort of information, photos, or videos of themselves or others without permission.**

CALL TO ACTION

Preventing online risks

- **Preventing risks to devices or to kids as they use the Internet starts with parents/guardians and the preemptive measures put in place in the household. Below is a checklist of action items to keep kids and their devices safe! Try bringing the family together to complete some of the tasks below, and engage in conversations:**

- **Set up parental controls on all devices and websites; these can include restricted access time, and parental notifications and alerts, when access to blocked websites are attempted.**

Tip! Bookmark common websites that kids visit for easy access, whether it's an educational game site or their favourite YouTube video.

- **Install pop-up and banner ad blockers so kids don't accidentally click on a bad one!**

Pop-ups or banner ads:
Advertisements that appear on websites or videos, they're either still images or moving/flash animations, however, sometimes they contain dangerous viruses!

- **Use safe search mode on an Internet browser, and encourage the use of kid-friendly search engines, such as Kiddle and Safe Search Kids, both powered by Google.**

Search Engine: A type of website that helps people find information on a specific topic that's available on the Internet.

- **Parents/guardians should educate themselves on the latest scams and news regarding device safety. Keeping up-to-date and being alert enables parents/guardians to teach kids. Kids should talk to a parent/guardian, or a trusted adult, about anything they're unsure about while using devices!**

CALL TO ACTION

Safe Internet browsing

- The Internet is where kids go to look at websites that have pages and pages of information, pictures and videos. They can learn a lot or be entertained for hours while on the Internet; however, it's important that they browse safely and/or with the supervision of a parent/ guardian, or trusted adult such as older siblings or educators.

- In order to protect kids while browsing, make sure they always ask a parent/guardian or trusted adult before using a device, and:

- **Do not click on pop-up ads or banner ads that appear on websites, as these can contain viruses, and request personal and private information.**

- **Avoid special offers and promises of free gifts, money and rewards. Nothing is truly free! Funny online quizzes and contests might be very tempting, but they're often being nosy, and require kids to enter information such as an email address, or connect to a social media profile in order to get the results.**

- **Prevent kids' devices, and the devices of others, from storing information for "auto-filling" at a later date. Often, devices will ask to "save" this information for convenience purposes, but this could potentially get in the hands of the wrong person!**

- **Be aware of fake websites. Scammers or "bad people" can create fake websites that look very similar to the real thing! Sometimes these have similar website addresses and logos, but they're actually trying to take kids' information or install a virus on their device.**

CALL TO ACTION

Downloading safely

- There's so much to download from the Internet, and younger kids may not even realize that what they're doing is considered "downloading".
- Pretty much anytime kids want to save something to their computer, tablet or phone, usually they have to download it first. Common examples are downloading new or updated versions of mobile apps, photos and videos they want to save for later, or electronic documents like e-books.
- A lot of what they download is free, and this may seem exciting – but, remember, not all that is free, is safe; and may contain viruses and malware.

To protect kids and their devices, it's recommended that they: Ask a parent/guardian fi rst, before kids download anything, to ensure that it's appropriate, and from a trusted website or verified game store.

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

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 activity themselves, and offer support when needed.

Phishing for Information!

- As we learned, scammers, or "bad people" on the Internet, often phish (pronounced "fish") for the personal and private information of others, in order to steal their identity, ask them for money, or put viruses on their devices.

- The information in this resource is meant to help you prevent being in situations where this can happen to you! With your new knowledge, colour in the pictures below the fish hook that represent ways that scammers can try and infect your devices and get your information! Then, match the method to the picture!

1. DOWNLOADS 2. EMAIL 3. VIDEO GAMES 4. TEXT MESSAGES

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