The image shows the cover of a spiral-bound notebook. The background is a bright yellow color with a pattern of small white dots. On the left side, there is a silver spiral binding. In the center, there is a large white speech bubble with a black outline. Inside the speech bubble, the text is written in a bold, comic-style font. The top part of the text is in yellow with a black outline, and the bottom part is in blue with a black outline.

**A GUIDE TO  
CYBERSAFETY**  
FOR GRADES 9-12,  
PARENTS, AND  
GUARDIANS

NationalCyberDay.ca



# BECOME A CYBERSAFETY SUPERHERO!

Apply these principles in order to become **#UnHackable!**

## **BE PRIVATE**

- Protect your information
- Use an 'online persona'
- Post and share sparingly
- Be extremely cautious with photos, videos, and webcams

## **BE SKEPTICAL**

- Verify if info sources are reliable or sketchy
- Recognize the signs of scams and fraud
- Limit interactions with 'online strangers'
- Regularly review your accounts for suspicious activity

## **BE SECURE**

- Secure your devices and accounts by keeping software up-to-date and not trusting sketchy apps
- Recognize signs of compromise
- Use password best practices

## **BE POSITIVE**

- Block and report bad behaviour
- Get help from a trusted adult when appropriate
- Interact with others in a safe and fun way

# SECURING DEVICES AND PROTECTING PERSONAL INFORMATION

## PASSWORD SECURITY

- Use a trustworthy password manager
- Passwords should be unique for each site and
- Should include a variety of numbers, characters, capitals, etc.
- Never store your passwords on shared devices or in your web browser
- Enable two-factor authentication

## ACCOUNT ACCESS

- Review any shared accounts
- Update account backup emails and contact info
- Remove any person you no longer want as your trusted contact

## BACK-UP

- Regularly back up the data on your devices to make recovery from a crash or hack much easier
- Use an encrypted or password protected physical storage device (like a USB stick) which can be more secure than online storage if kept safe

## SHARED DEVICES & WIFI

- Remember to log out of your accounts if using a public device such as at work, school, or library
- Never save passwords to devices that are shared
- Be cautious using public WiFi when accessing sensitive accounts or entering personal information

## APP SETTINGS

- Delete apps you don't recognize from your devices
- Review the permissions of each app, check access to: location, microphone, camera, notes, documents, and photos
- Ensure that apps do not operate in the background and those that require connectivity request it every time

## PRIVACY SETTINGS

- Ensure posts and accounts are set to 'private'
- Check how your primary account 'looks' to the world and what the public can see
- Review all privacy settings on your phone and devices including online data storage and backups (like iCloud)
- Check the Find My settings (or others) to see if your location is shared with anyone

## SOFTWARE

- Never disable built-in antivirus protection
- Consider supplementing with adblocking browser extensions and antikeylogger tools
- Run system updates as soon as possible

## DEVICE SECURITY

- Make a list of all devices including: phones, laptops, tablets, security cameras, smart TVs, etc.
- Ensure each device is configured with a custom, unique password or PIN and a locking screen saver
- Be sure to enable automatic updates when possible

## YOUR HOME NETWORK

- Change the default name and password on your router
- Make a "Guest Network" on your router for your smart devices like speakers, thermostats, alarms etc.

## CHECK-IN

- Regularly review your accounts and devices for suspicious activity and log-ins (if technology permits)
- Watch for new icons, installed apps, and system tray icons that you do not recognize
- Use Virustotal to check on suspicious files and websites

# INTERNET SAFETY BASICS

## WHAT ARE COOKIES?

**Cookies** are the files that get created when you visit a **website**. The cookie is created on your web browser so the website can recognize you in the future.

Cookies can include your **name, address, pages you've browsed, contents of your shopping cart**, or information about **which pages** on the site **you visited**.

## HOW TO BLOCK COOKIES

Programs like Privacy Badger are browser add-ons that prevent companies from tracking your online activities



Download for your web browser and add the extension



Click on the extension icon when required to manage cookies

## DO I HAVE TO ACCEPT COOKIES?

**No!** The information collected by some cookies is both a **privacy** and a **security risk**.

## IF I DON'T ACCEPT COOKIES, WHAT WILL HAPPEN?

**Most websites will still allow you in**, although you may not have access to the entire site's functionality.



**FEAR, URGENCY, SECRECY**

**PERSONAL INFORMATION**

**AUTHORITY OR LEGITIMACY**

**PAYMENT (IN ANY FORM)**

## RECOGNIZING SCAMS

Scammers can fake any number and any organization



### #UNHACKABLE TIPS

Don't trust your call display!



### DON'T OPEN ATTACHMENTS FROM UNSOLICITED EMAILS

There is **no safe file type**. malware can be embedded in JPEGs, PDFs, PNGs, etc.

## WHAT IS MALVERTISING?

- Scammers invest in paid newsfeed ads
- Victims are lured with personalized tech support scams

## PROTECT YOURSELF!

- Be wary of online ads, even from familiar brands
- Make your antimalware updates automatic
- Only use ad-blockers you fully trust

## CONFIRM YOUR PROVIDER'S INFO

Verify the phone number and website on the back of your payment card or invoice.

## CHECK THE URL

Scammers may use shortened URLs (such as bit.ly or buff.ly) to redirect to their fraudulent website, or to a URL that closely mimics a legitimate company's website.

# SOCIAL MEDIA MANAGEMENT

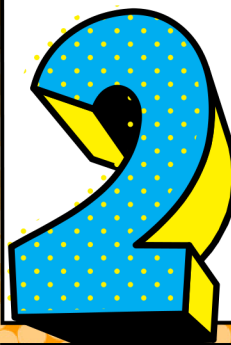
Most social media platforms are **13+** but many kids sign up **much younger**. Do you know the age requirements for **your child's** apps?

## MUST-KNOWS FOR CHILDREN ON SOCIAL MEDIA



### **WHAT YOU PUT ONLINE, STAYS ONLINE**

Even things you delete can be saved or screenshotted, including those Snapchats meant for just one friend.



### **ONLINE STRANGERS ARE STILL STRANGERS**

If you wouldn't tell something to a stranger on the street, don't tell your online 'friends' and contacts.

### **BE AWARE OF THE OVER-SHARE**

It can be easy to over-share on social media, especially if you forget who can see your profile.



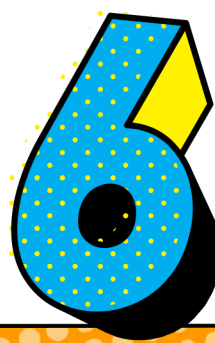
### **PRIVACY IS POSSIBLE!**

Forums and group chats can be a great way to connect, but don't feel pressured to share more than you're comfortable with.



### **USE PRIVACY SETTINGS**

Every platform has privacy settings, make sure you know how to use them. Make your account private and secure.

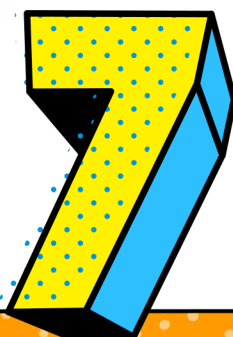


### **REPORT OR BLOCK**

Ensure you know how to report and block both users and content on every account that you use.

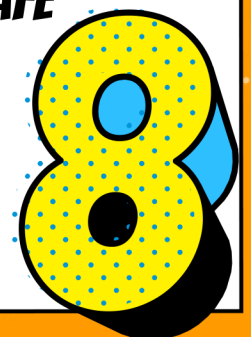
### **UNPLUG AND TURN OFF**

You don't need to be on social media all the time! It's okay to take a break, and you don't need to take part in every conversation.



### **YOU DESERVE TO FEEL SAFE**

Don't hesitate to block anyone who makes you feel uncomfortable and talk to someone you trust if this happens.



# TALKING SOCIAL MEDIA WITH KIDS!

## TIPS TO KEEP SOCIAL MEDIA CONVERSATIONS POSITIVE



Have **regular conversations** with your children about the internet and social media from a **young age**

**Checking in** with your child for a minute or two about their online experience can make a **huge difference!**



### Talk about your own experiences online, good and bad

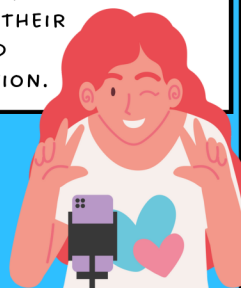
ENCOURAGE THEM TO USE THE INTERNET IN A POSITIVE WAY, TO RESEARCH THINGS, TO DO HOMEWORK, TO TALK TO FAMILY, AND TO LEARN ABOUT THE WORLD.



TEACH YOUR CHILD ABOUT THE IMPORTANCE OF PRIVACY SETTINGS AND THE POTENTIAL RISKS ASSOCIATED WITH SHARING PERSONAL INFORMATION ONLINE.



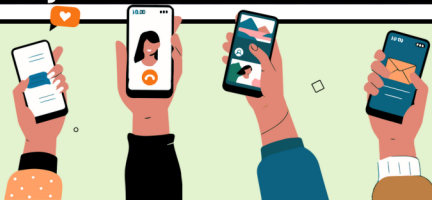
HELP THEM UNDERSTAND HOW TO SET THEIR PROFILES TO PRIVATE, AND LIMIT WHO CAN VIEW THEIR POSTS AND INFORMATION.



KEEP YOURSELF INFORMED ABOUT THE LATEST SOCIAL MEDIA TRENDS, FEATURES, AND POTENTIAL RISKS.

### Ask your child about the apps and websites they use

MANY PARENTS FEEL LIKE THEY DON'T UNDERSTAND THE LATEST TECHNOLOGY, APPS, OR SOCIAL MEDIA THAT THEIR CHILD IS USING.



ASK YOUR CHILD TO SHOW YOU THEIR FAVOURITE APPS, GAMES OR WEBSITES THIS WILL HELP YOU UNDERSTAND HOW THEY WORK SO THAT YOU CAN TALK ABOUT THE POSITIVES AND WHETHER YOU HAVE ANY CONCERNS.



IF YOU THINK ANYTHING YOUR CHILD IS ACCESSING IS NOT APPROPRIATE FOR THEIR AGE, BE READY TO EXPLAIN WHY.

WHEREVER POSSIBLE, MAKE IT A JOINT DECISION WITH YOUR CHILD. THIS WILL HELP THEM TO UNDERSTAND THE REASONS NOT TO USE SOMETHING, AND MAKES IT MORE LIKELY THAT THEY WILL STICK TO IT.

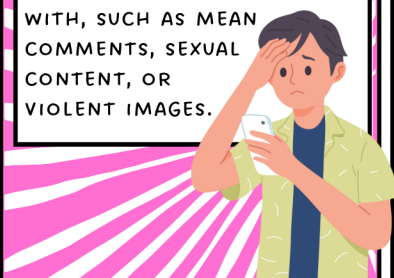


### Reassure them that they can always talk to you

MOST CHILDREN ARE CAUTIOUS ONLINE.

OFTEN WHEN THEY COME ACROSS UPSETTING CONTENT IT'S BY ACCIDENT, OR BECAUSE SOMEONE SENT IT TO THEM.

ASK THEM IF THEY'VE SEEN ANYTHING ONLINE THAT THEY ARE NOT COMFORTABLE WITH, SUCH AS MEAN COMMENTS, SEXUAL CONTENT, OR VIOLENT IMAGES.



IF THEY ARE UPSET OR WORRIED ABOUT SOMETHING THEY'VE SEEN, TALK ABOUT HOW THEY FEEL, AND HOW THEY CAN AVOID SEEING SIMILAR THINGS IN FUTURE.



IF NECESSARY, HELP THEM TO REPORT OR BLOCK CONTENT THEY FIND DISTURBING

STAY CALM IF YOU FIND THEY'VE COME ACROSS SOMETHING YOU DON'T APPROVE OF. MAKE TALKING WITH YOU A SAFE SPACE.



# MISINFORMATION ON SOCIAL MEDIA

## MISINFORMATION

Social media has **both positive and negative implications**. One of the negative results of social media is the abundance of misinformation circulating on the internet. **Protect yourself by using the C.R.I.S.P. scan!**

## THE C.R.I.S.P. SCAN

- C** Consider the source
- R** Read beyond the page
- I** Investigate the clues
- S** Scan for bias
- P** Proceed with caution

Here's how misinformation quickly spreads on social media

WHEN A SMALL AMOUNT OF INFORMATION IS AVAILABLE, THE TRUTH IS SHARED MORE OFTEN.



HOWEVER, WHEN LOTS OF INFORMATION IS AVAILABLE, SOCIAL MEDIA USERS EXPERIENCE INFORMATION OVERLOAD.



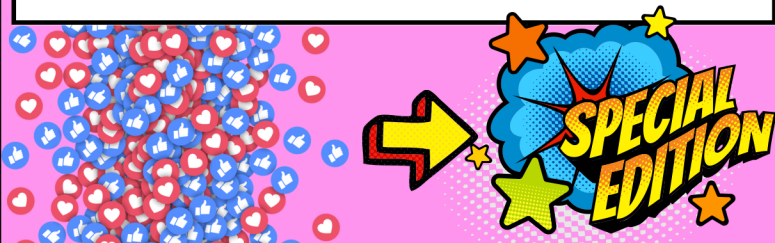
INFORMATION OVERLOAD CAUSES PEOPLE TO SHARE INFORMATION INDISCRIMINATELY, WITHOUT CHECKING IF IT IS TRUE OR FALSE.



VIEWERS GET AFFECTED BY THE EMOTIONALLY SHOCKING INFORMATION, PARTICULARLY EXAGGERATED HEADLINES.



SEARCH ENGINES AND SOCIAL MEDIA PROMOTE THE MOST ENGAGING AND RELEVANT CONTENT FOR EACH USER.



COGNITIVE AND SOCIAL BIASES ARE REINFORCED, MAKING USERS MORE VULNERABLE TO MANIPULATION.



# ONLINE CRIMES

If you or someone you know has been **victimized** by online harassment, cyberbullying, sextortion, or human trafficking, **here are some ways to seek help.**

**Victim Services of Durham Region**  
Phone: 1(888)579-1520 ext. 3400

**Victim Services Toronto**  
Phone: 416-808-7066

**Kids Help Phone**  
Text: CONNECT to 686868  
Call: 1-800-668-6868  
NeedHelpNow.ca

**Canada's National Human Trafficking Hotline**  
1-833-900-1010

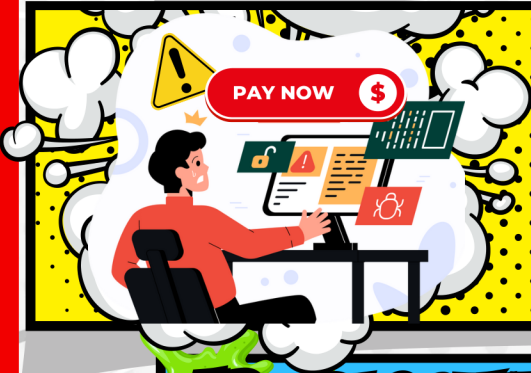
## SEXTORTION

The act of extorting payment by threatening to reveal intimate images or videos, OR making threats of various kinds in order to receive intimate images or videos



## EXTORTION SCAMS

Extortion scams can take many forms, but they all have one thing in common... Paying the scammer usually leads to increased threats and demands.



## AD-BLOCKING SOFTWARE

Provides improved security by blocking third party trackers, malware, and more. Makes browsing faster, more private, and keeps you safe from malicious ads!



## MALICIOUS APPS

Malicious apps are software secretly installed on your device that cause harm. They consist of viruses, spyware, ransomware, and other unwanted software that exploits your device and/or personal data.

