



# Privacy and cyber-safety for families

Dec. 7<sup>th</sup>, 2024

CyberSafety

Nicole Stephensen and Takaya Terakawa



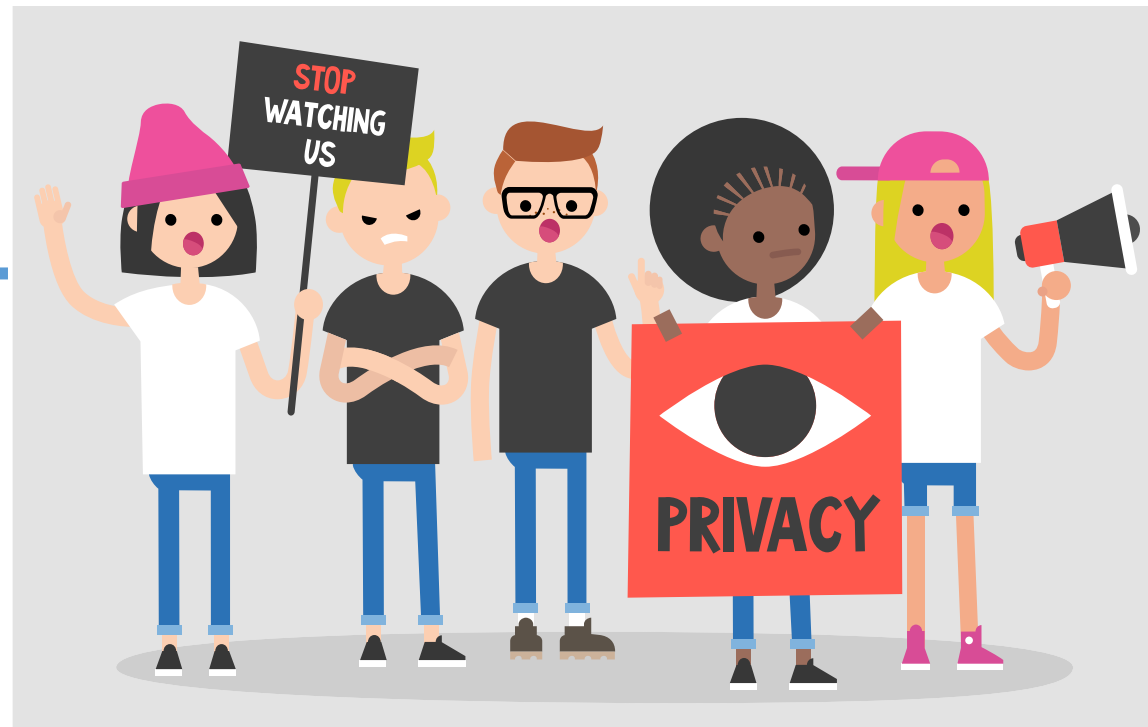


# Today's agenda

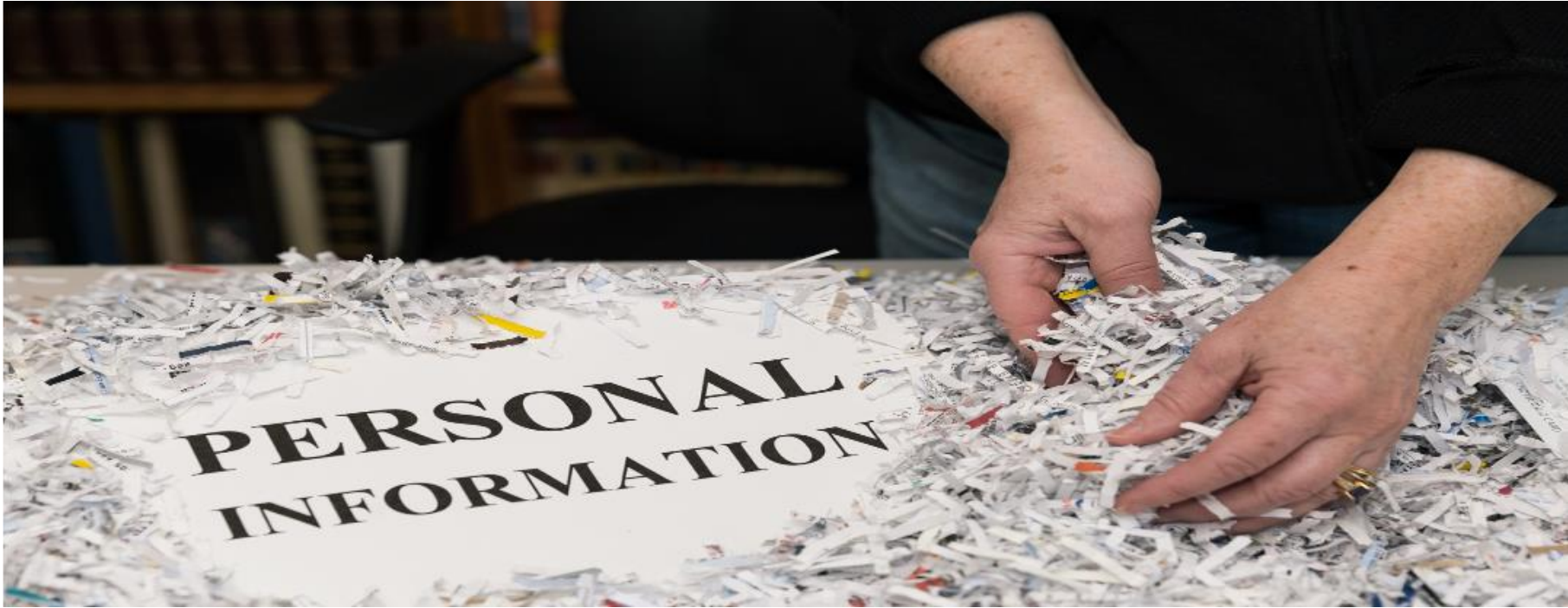
---

- Understanding 'privacy'
  - Personal information
  - Risks facing children
- Understanding 'cyber-safety'
- Privacy & cyber-safety issues in the current digital landscape
  - Online grooming, online bullying, sharing nudes, gaming addiction, harmful content
- Our roles as educators, families, parents
- Your family cyber-safety plan
  - Common apps for parents to keep an eye on

# Understanding 'Privacy'



?



# What is Personal Information?



# The environment surrounding children and the risks they face

---

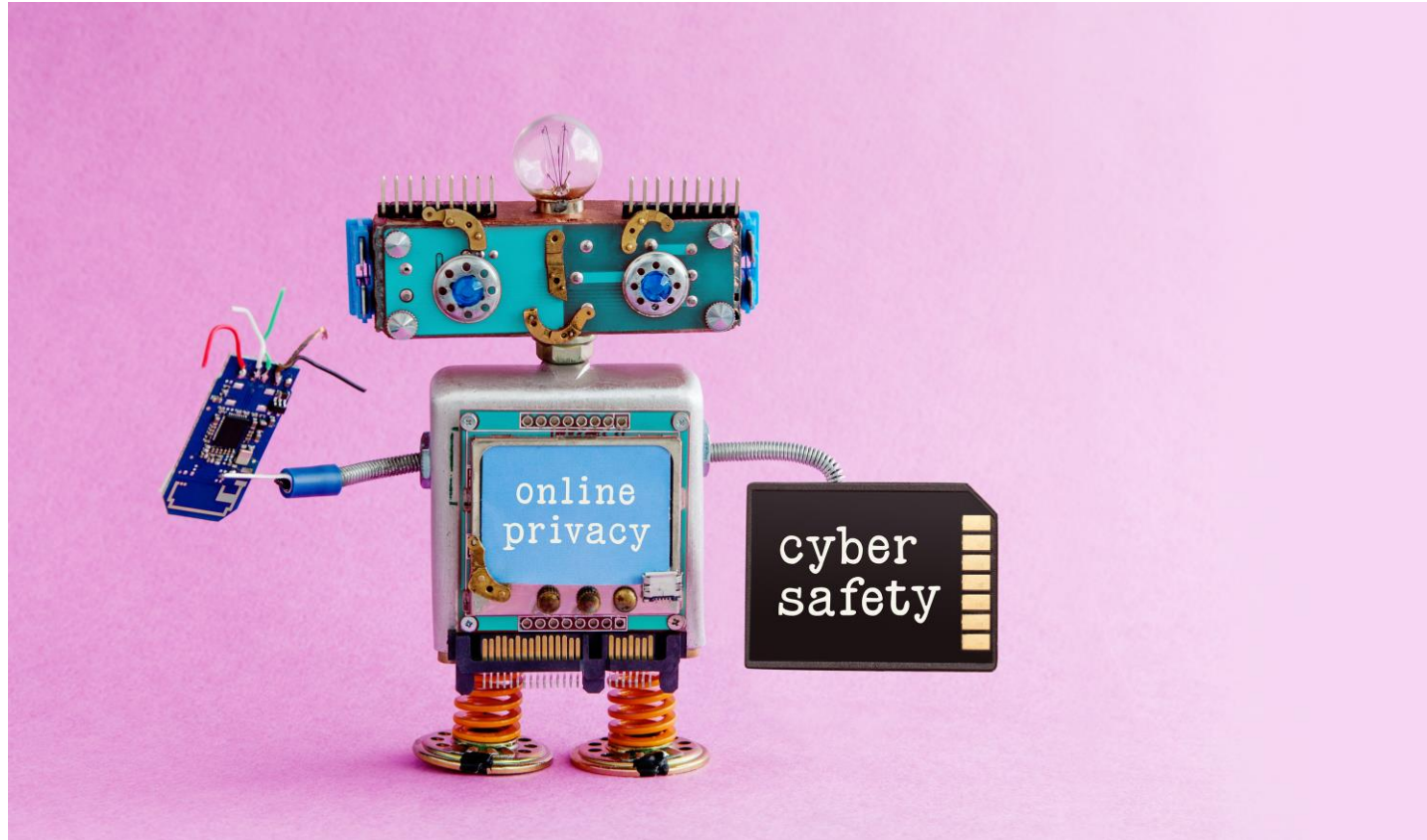
- Children can connect with millions of people around the world
  - through websites, applications (Apps), and online games
- Online has become a hunting ground for those adversary actors
  - Teenagers often do not realize that personal information disclosed online is accessed by much wider audience
    - This often leads to unexpected and undesirable results

# What cyber-safety means

**Privacy** – protect your personal info

**Security** – controls to protect any info (**Cyber** = online)

**Safety** – being protected from danger, risk, injury



# In today's digital era, children are spending more time engaging online to...

- Complete school assignments
- Attend extra classes
- Connect with family
- Socialise with their friends
- Play online games
- Buy things



**CYBER  
SAFETY**

# Privacy and cyber-safety issues right now

In the current digital landscape, family members are spending more time online. Here are some things you should be mindful of ...

## Privacy issues

1. A bigger digital footprint
2. Increased personal information given online and through apps
3. More time spent in gaming and chat rooms

## Cyber-safety issues

1. Increased activity by cyber criminals
2. Passwords being re-used/compromised
3. Increased cyber-bullying





# Online Grooming

**Definition:** The act of becoming friendly with someone over the internet and gaining their trust. It is often done as a prelude to sexual contact with children.

- Target Identification:
  - Perpetrators seek out vulnerable children on social networking sites, such as those sharing illustrations or discussing personal struggles.
- Building Rapport:
  - They initiate conversations with kind words and empathy to establish a connection and gain trust.
- Daily Interaction:
  - Through consistent, daily communication, they reduce the child's initial wariness and foster a sense of trust.
- Exploitation of Trust:
  - Once trust is established, perpetrators make inappropriate demands, such as requesting explicit photos or arranging in-person meetings.
- Manipulation:
  - Children, now emotionally dependent and trusting, may feel unable to refuse these demands, fearing rejection or disappointing the perpetrator.

This underscores the importance of educating children about online safety, recognizing manipulation tactics, and encouraging open communication with trusted adults.

CYBER  
SAFETY



# Online Bullying

**Definition:** Cyberbullying is bullying that uses digital technology

- Cyberbullying occurs through interactions on social networking sites, messaging apps, game apps, and mobile phones
  - Act of frightening, angering, or embarrassing others

## Examples:

- On social media, spreading hurtful words, false information, or posting embarrassing photos
- On messaging platforms, sending messages that hurt or threaten someone
- Pretending to be someone else and sending malicious messages to someone else

Bullying in real life and cyberbullying often happen at the same time



# Sharing Nudes

Self-taken photo victimization is a form of child pornography in which children under the age of 18 are threatened and forced to take and send photos of themselves in their underwear or naked via smartphones or other devices.

- A significant age gap
  - Might be in a relationship
- Frequent contacts
  - Providing a lot of support, so children have a trust in perpetrators
- Don't know about the risks involved in sending self-taken photos
- Feel like not being cared and accepted by parents
  - Loneliness
  - Psychologically want to keep the perpetrators who asked to take photos

Not only “she” but “he” also could be a victim



# Game Addiction

**Definition:** A condition characterized by severely reduced control over gaming habits

- resulting in negative consequences in many aspects of the life, including self-care, relationships, school and work

## Symptoms:

- Unable to control the amount of time or frequency of gaming
- Make gaming the top priority in daily life
- Continue to play games even when problems occur
  - let the issues escalate, still gaming



# Harmful Content

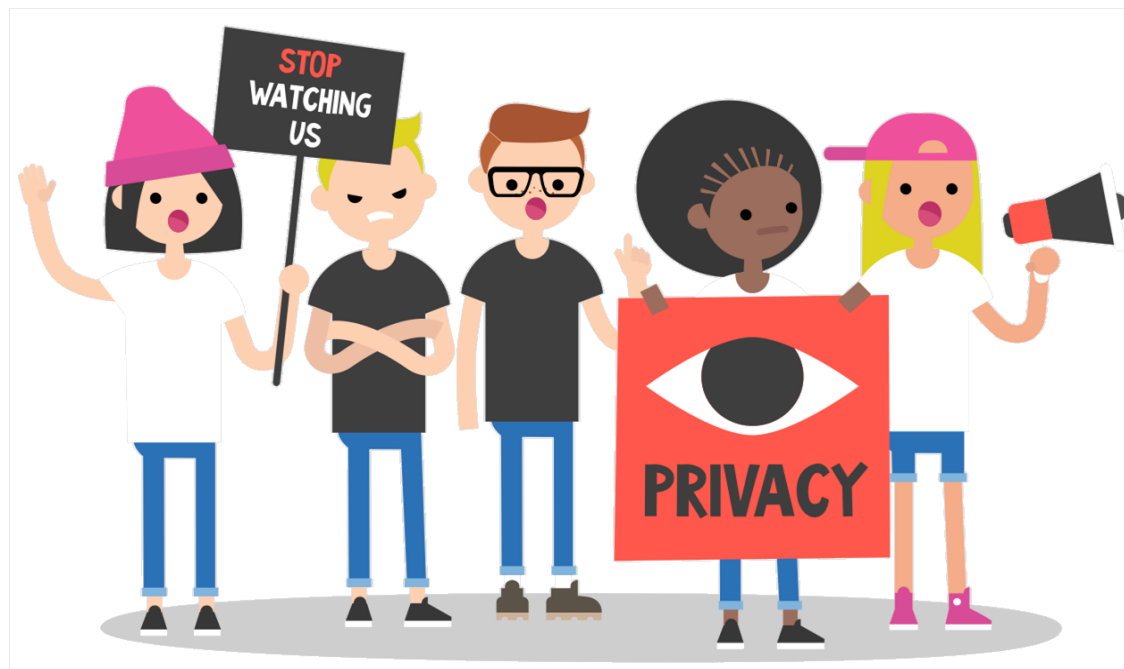
---

Cyberspace and real world are the same!

- Dangerous places, including
  - Adult sites, suicide sites, illegal part-time work
    - Children are targeted and trapped without even recognizing being trapped

Children have limited ability to perceive risk and predict outcomes

# What are our roles in addressing children's privacy and cyber-safety challenges?



To address  
cyber and  
privacy issues  
consider making  
a  
**Cyber-safety  
Plan**



# Your Family Cyber-safety Plan



## 1. Take a family-tech inventory

- Communication devices (e.g. mobile phones, tablets, laptops)
- Gaming devices (e.g. PS4, VR)
- Smart TV, home assistant (“hey Google!”)
- Smart toys and surveillance devices (e.g. baby monitor)
- Connected home appliances and gadgets (e.g. Smart fridge, smart watch)



# Your Family Cyber-safety Plan



2. Think about what the tech does, how it helps you, what it captures

- Help you communicate with others?
- Send you stuff you asked for/ didn't ask for?
- Capture images of you or someone else?
- Record what you're doing in your home?
- Allow you to spend \$\$ ?
- Ask you for (or collect behind the scenes) your personal info?
- Understand your likes/ dislikes/ tastes/ favourites?

# Your Family Cyber-safety Plan



## 3. How are you actually using the tech?

- Anyone outside the fam using your tech? (e.g. Nana, babysitter)
- Files stored on the tech? (e.g. images, work, school-work)
- Working from home or home-school?
- Apps from school?
- A lot of unsupervised screen time (or just a little)?
- Shared devices or family-sharing via the cloud?
- iTunes account? PayPal? Online banking?
- Passwords
- MultiFA

# Your Family Cyber-safety Plan



## 4. Know your pain-points and options

- Review accounts, apps, games – apply privacy, security and safety settings (**BIG job... try doing 2/ night for a month**)
- Consider content filters/ restrictions for kids (YouTube vs. YTKids... big difference in content!)
- Tech-crazy kids – Using it alone? Worried about friendships? Unhappy unless online? Safe?
- Virtual currency (e.g. gaming money, skins) – a regular ask from kids?
- Phishing/ scam emails, texts, instant msgs

# Pain-points: really look closely at apps... for fun, and from school



## TikTok

*Social media app for creating, editing and sharing short videos. Users can follow, like and comment on videos, live stream videos, and easily repost videos to other platforms.*



## WhatsApp

*Messaging app that allows users to send texts, send photos, make calls and video chats worldwide using an internet connection. It also allows the user to share their location.*



## Snapchat

*Popular app where users can take a photo / video that disappears within 24 hours. The app also allows viewers to message, video chat and share location information.*

# Your Family Cyber-safety Plan



## 5. Communicate needs and rules

- Delete accounts, apps, games you don't use
- Accounts linked to your \$\$ - for adults only
- Password hygiene
- Bookmark 'scamwatch' sites, and haveibeenpwned in your browser
- NO online chat
- 'Trusted adult' – let your kids choose one other than you (teacher, family friend, godparent, aunty/ uncle)
- Stop, block, tell rule for cyberbullying
- Is it worrying or weird? Show me, I'll help
- Use tech in common areas, not bedrooms

# Your Family Cyber-safety Plan



6. Stick to your rules and refine them as you grow (smarter, safer and 'up'!)

- Know what's going on (e.g. some fun cartoon games are not safe for kids!)
- Self-check - do you need additional [away-from-screen time](#) together?
- Ask your kids to choose their own privacy settings (with you as guide), give praise for sticking to the rules, and trust in them (it's a powerful motivator)
- Talk to other parents about what they are doing
- Get older teens involved – they can teach YOU so much!

CYBER  
SAFETY

THANK YOU