

Online Safety Webinar Series

Session 3 for Adolescents:

Technical Online Safety *Do's and Don'ts*



AutismONTARIO
see the potential

Our Presenters

Sarah Southey, MSW, RSW

Nicole Lisi, BA, MSW Student

Katie Sedej, Self Advocate



Content

- Reflags (abuse, exploitation, etc.)
- Privacy functions
- Revealing information
- Meeting “online” friends
- Spam emails
- Online purchases
- PLAY IT SAFE





Red Flags

- If they ask you to do things like show your naked body, ask for money or gifts, do inappropriate or unsafe activities, share personal information, etc.
- If you don't know them and they have inappropriate pictures
- If they facetime you and you don't know them
- If they have no picture and no posts
- If they make fun of you
- If they are a stranger and they ask you to join a group chat
- If they offer you free products
- If they start a conversation in a sexual way
- If it's someone who is a lot older than you



"PRIVACY

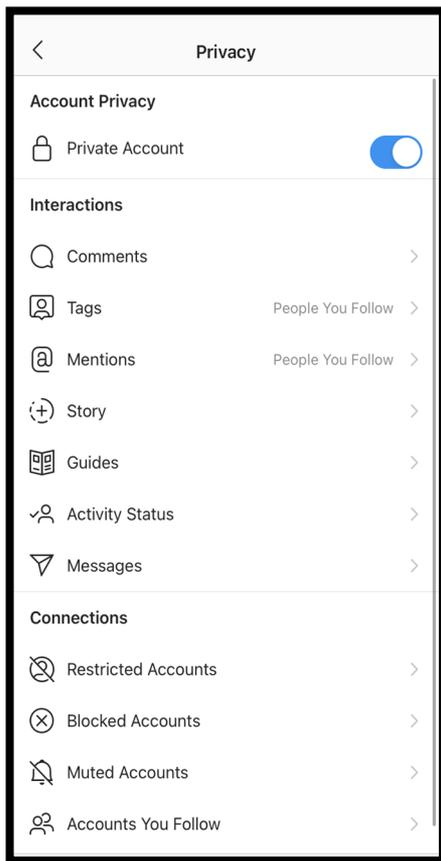


SETTINGS"

memegenerator.net

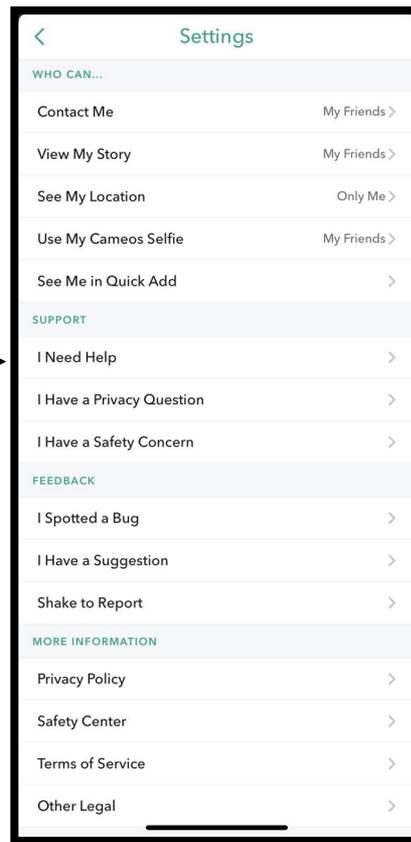


Privacy Functions



← *Instagram*

Snapchat →



Sharing Personal Information

DO NOT SHARE LIST:

- Address
- Financial Information
- Passwords
- Where you work or go to school
- Details on your schedule

<https://jccrsblog.wordpress.com/2017/03/05/your-privacy-in-the-book-of-your-face/>





Meeting “Online Friends”

- Consider the difference between “friend” and “acquaintance”
- Think about if the relationship is reciprocal
- Think about how you can safely talk to them
- How does your new friend make you feel?
- If you plan to meet in person with someone you’ve met online, make sure you tell someone your plan and meet in a public place



Spam Emails

- If a bank asks you to “verify” something over email, it’s a major red flag. A legitimate financial institution will never ask you to verify or confirm anything through an email or link.
- If you don’t recognize the destination URL, it’s probably not legitimate. It might have your bank name in it or even have a .com domain, but look for little differences that you don’t regularly see on the actual bank page.
- Something as simple as a grammar mistake can give up a phishing email.

[email-phishing-signs-to-teach-your-teens](#)



Online Purchases

- Use familiar websites
- Look for the lock icon or https url (https is secure vs. http is not secure)
- Don't overshare
- Check your debit and credit card statements regularly
- Make sure you have an antivirus program or other anti-malware tools on your computer
- Avoid shopping online in public
- Do your research on retailers



Bringing it all together

P Personal information - don't share it

L Let a trusted adult know - tell someone if anyone asks for your personal information.

A Attachments - beware before opening any attachments.

Y Your feelings are important - if something happens that makes you uncomfortable, tell an adult right away.

I Information - remember that not everything you see online is true. If you are unsure ask a trusted adult.

T Take breaks from the computer.

S Spending money - don't buy things online without permission.

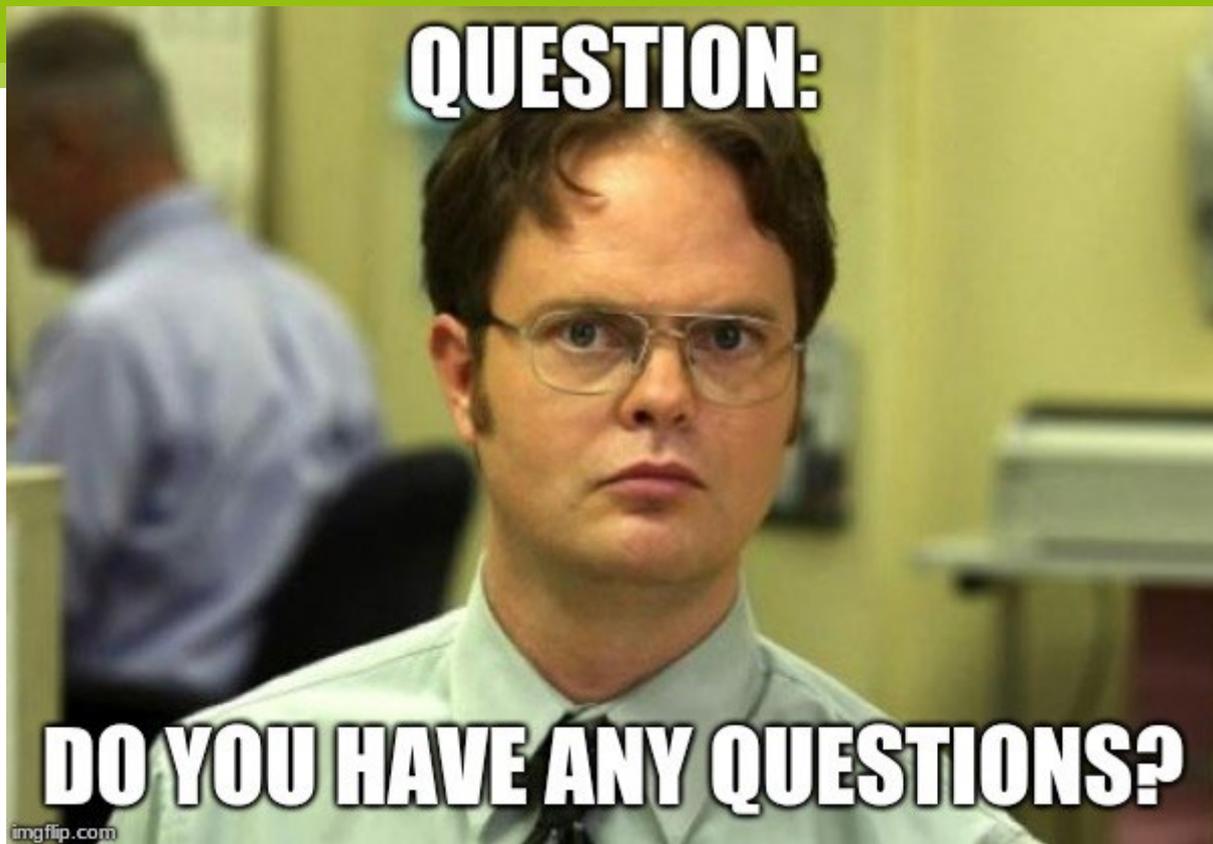
A Act politely - don't say anything online that you would not say to someone in person.

F Friends online should stay online.

E Enjoy yourself.

Adapted from: <https://csesa.fpg.unc.edu/sites/csesa.fpg.unc.edu/files/Internet%20Safety%20for%20Adolescents%20with%20Autism.pdf>





Future Sessions

- ❑ Session Four: Social Safety and Positive Interactions For Adolescents – Reading the Room

REGISTER HERE: <http://bit.ly/Webinar-Cyber-Safety>



Additional Resources

Internet Safety for Teens with Autism Resource:

<https://csesa.fpg.unc.edu/sites/csesa.fpg.unc.edu/files/Internet%20Safety%20for%20Adolescents%20with%20Autism.pdf>

A helpful online safety guide for people with ASD:

<https://thetouchpointsolution.com/blogs/touchpoints-blog/a-helpful-online-safety-guide-for-people-with-autism-spectrum-disorders>

Be Internet Awesome by Google:

https://beinternetawesome.withgoogle.com/en_us



Contact

Sarah Southey, MSW, RSW

sarah.southey@redpathcentre.ca

www.sarahsouthey.com

