

# Back to-school security

## Cybersecurity for students

As students return to school, parents need to know how to protect their children from cyber-risks in an evolving digital world.

## What cyber-risks do kids face? How can we help?

### Cyberbullying

Cyberbullying is a type of bullying that happens online. It can happen in an email, text message, app, online game or social media site. Bullies send harassing or cruel messages and encourage others to do the same.

Talk to your family about cyberbullying and how they should handle it. If a child in your life is at risk, suggest talking to their parents or guardians and trusted school staff. This is also a good time to check the security settings on their apps.

### Phishing

A phishing attack might look like a real email or text message, but it contains a malicious link or intent to steal sensitive information.

Children and young adults might not be able to recognize a phishing attack. Talk to them about ways to distinguish between real and fake messages. Tell them to look at the sender of the message and think critically about whether it could be a trick before doing

anything.

### Privacy settings

Privacy settings are an important first layer of defense for keeping our information secure.

By implementing high privacy standards, you can prevent personal data from being exposed. It also reduces the amount of information about you online.

This is also a critical time to discuss online friends, followers, and other individuals they interact with over the internet.

### Consent to photos

Photos posted online without someone's consent increases digital exposure and could lead to identity theft.

Check with your student's school about their photo policy, and always follow up on removing unwanted information online.

### Interacting with unknown people

Stranger danger is real and extends to the virtual world! Online predators have the luxury of anonymity.

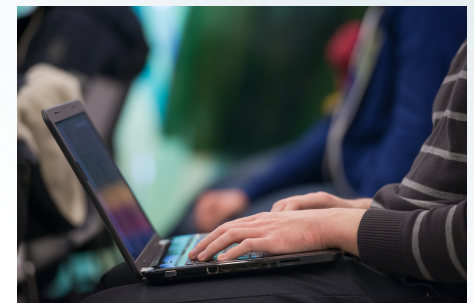
It's critical to know what your student is doing, who they are interacting with and what they can access online. Staying aware and educating yourself and your child will help protect them.



## Digital citizenship

A good digital citizen practices safe, legal and responsible use of technology. Here are a few tips for your child or students on how to be good digital citizens:

- ! Get permission from a parent or guardian before making online purchases
- ! Spend time away from devices
- ! Always treat others with respect
- ! Avoid all suspicious online communications, including email, texts and ads
- ! Keep your apps and devices secure with strong security settings and passwords



## Cyber quiz!

After discussing with your child or student the importance of being cybersecurity, test their knowledge with this quick quiz:

### Q1: Why is a strong password important?

- a)! It stops someone from accessing your account
- b)! It allows you to tell your classmates something about you
- c)! Passwords are not important

### Q2: What is phishing?

- a)! Asking your friends for password suggestions
- b)! A fake message with the intent to steal information
- c)! A marketing email from a local store