K-12 Cybersecurity: Keep Kids Secure from Kindergarten to Graduation

Nowadays, kids aren't just polishing apples and stuffing their bookbags before heading to school, they're firing up laptops and using video chat with their teachers.

Actually, most parents today probably had computers when they were in school, but technology has become even more critical. And the trend toward more tech-heavy schools only accelerated due to the COVID-19 pandemic.

With all the gadgets and gizmos, though, come security risks. You may have seen some recent high-profile incidents where school districts were struck by ransomware. Schools are as reliant on computers as any other 21st Century business and kids use multiple online accounts and devices to learn.

But with so many hackers and cyberbullies on the web, what's a kid to do? How can parents, teachers, and administrators keep cybercriminals out of the schoolyard? Hopefully, this guide to help you learn to stay safe online every semester (and even over the summer)!

Show your school spirit with a strong password

In the serious endeavor of school cybersecurity, the first way to score big is to have a strong password! Just like your school team's mascot, a strong password is how you can show off your school spirit and keep your accounts safe from the poor sports of the web known as hackers.

How do you create a championship password? Always think three words: unique, long, complex:

- Unique: Use a different password for each account and never reuse passwords. This way, if one of your passwords gets stolen, your other accounts can't be cracked. How do you remember all those passwords? Use a password manager – many devices and web browsers have them built in!
- Long: Every one of your special passwords should be at least 12 characters long.
- Complex – Each unique password should be a combination of upper and lower case letters, numbers and special characters (like >,!?).

You don't want a password that is easily guessable, such as "012345," "password," or your birthday. Ideally, your password shouldn't include recognizable words at all. This is why using a password manager can help you turn pro in your cybersecurity career.

The ABCs of Online Learning: Always Be Cybersecure

Even as the COVID-19 pandemic moves to the background, it seems online learning is here to stay for many of us in one form or another. Unfortunately, all those devices, home networks, and accounts can leave schools vulnerable. To stay safe while learning online:

1. Activate automatic updates for your devices and software.
2. Be cautious with links and attachments — think before you click to avoid phishing attacks.
3. Create strong passwords for each of your devices and accounts.
4. Don't share personal information with people you meet online.
5. End using the default password for your home internet router — change it to something unique, long, and complex instead!
6. Frequently back up your files — then you don't need to worry about your homework if your dog eats your laptop.

The online library is always open

Fortunately, for bookworms with an internet connection, the web's library of information never closes. However, without a helpful librarian at the front desk, it can be a little tough to understand what knowledge is golden.

- **Citation needed**: Try to verify the information you use in your studies. Official government websites (with .gov web addresses), trusted news outlets, and websites ran by universities (.edu) are good. When using an online database like Wikipedia, check out the sources at the bottom of the page. If you need to check if your online research is reputable, talk to your teacher!
- **Share with care**: When you're hitting the online books, you might be asked to share. Be very cautious about filling out forms and providing personal information (like your name, address, and birthdate). We recommend that you only provide what is necessary and talk to a trusted adult if you have questions.
- **Watch out for the phishing hooks:** Cybercriminals will use deceptive emails or messages to lure you into revealing your personal information, like your passwords. Don't take the bait! Stay vigilant and double-check the sender's legitimacy before clicking on any suspicious links. If you don't know the sender, show the message to an adult you trust.
- **Shhhh…know the copyright rules**: Just like you can't photocopy an entire book without permission, always respect copyright laws when using online resources. Cite your sources, give credit to the original creators, and avoid plagiarism. This goes for artificial intelligence programs, too. Don't think you can get away with copy and pasting. Believe us, teachers can tell.

Block the bullies

Sometimes cyberbullies show up on the digital playground. They might be looking to take your lunch money, but often their goal is to make you feel bad about yourself. If a joke or other form of online attention makes you feel bad and those making the joke won't stop after you ask them to, this is a form of cyberbullying, and you should talk to a trusted adult. Hurtful comments online can have a real impact on your mental health – if you feel like hurting yourself, you should reach out to someone immediately.

Many kids and teens find it extremely helpful to block cyberbullies online – every platform has simple ways you can block and report users engaged in bullying behavior. There's no shame in having a strong blocking game!

New tech, who dis?

It might feel like you have to be a tech wizard these days to guide your little learners through their education. But it's fine if you aren't a tech-savvy parent! If you need help, reach out to other parents or your child's school. If the school issues or requires technology that you or your child are not familiar with, explore its features together. Remember to configure the security and privacy settings together right away.

Help others stay safe online

Help others in your school system stay safe online. Consider giving a presentation about cybersecurity basics at school – there are tons of resources, including PowerPoint presentations aimed at different age groups.

Additional Resources

- K-12 Online Learning
- K-12 Education Leaders' Guide to Ransomware: Prevention, Response, and Recovery