Virtual schooling: 11 ways to keep your child safe online

September 2020

Take a look through our back-to-school checklist to help you, as a parent or guardian, make sure your child stays safe while learning online.

The start of a school year often means sharp new pencils, new classes, and new routines. This year, the ongoing COVID-19 pandemic is rocking school districts with different rules and learning structures. Some students are getting their education entirely online, some will have a mix of virtual and in-person learning, and some will be physically attending all their classes. No matter which form your child's return to school takes, chances are they'll have to engage with their education online in some way. Follow these steps to keep them safe.

1. Remove smart assistants during school time

Your smart assistant is always listening for a "wake" word, which means it can listen in on your child's classes and conversations with their friends. Ask your child to turn off the voice assistant on their laptop, tablet or phone. If you would like to delete recordings, you can do that on Amazon Echo, Apple's Siri, and Google Homedevices.

2. Use a password manager and unique passwords

Your child may use multiple services on their laptop, tablet or phone. Encourage them to use unique passwords and a password manager. This means they only have to remember one password to access all the other unique passwords that allow them to access their accounts across all devices. You and your child can learn more about different password managers by searching online, and by reading articles here, here, and here.

Passwords shouldn't be easy to guess, or contain personal information such as pets' names. They shouldn't be too short, as that can also make them easier for bad actors to crack. Using the same password for all services can put your child's information at higher risk of hacking. It's significantly easier for bad actors to access accounts when they all have the same password. Remind them to never share their password with anyone.

3. Maintain primary email accounts

Explain to your child that maintaining their primary email account is important because many services use that address as their account username, to communicate password resets when a password is forgotten or lost, and to identify them. If their account is hacked, a bad actor could use that access to take over their other accounts, including gaming personas, and even impersonate them on social media. Use a strong password and avoid using services that automatically delete email accounts after a period of inactivity. Remember to change the email address for all your child's accounts before you switch to a new email address.

4. Use two-factor authentication

Some schools may already use two-factor authentication for some services, but you can also check out which services allow you to add this extra layer of security. The best options are authenticator apps and physical authentication tokens that your child can plug into their computer as a USB key.

5. Seek out services with strong encryption

School districts will often choose the services used for schoolwork, but you can also have a say in making sure that your child uses other services which offer strong encryption. They can use end-to-end encrypted messaging services to communicate with classmates. Encourage them to only communicate in closed groups with friends, and to report any unwelcome messages. Remind them that what they post might be copied and forwarded without their permission, or even used against them. Search online to see which services offer end-to-end encryption.

6. Choose a browser and search engine that respect privacy

Children may spend a lot of time browsing the Internet for their school projects, and to explore what's available online on a more personal level. Part of that searching is about discovering who they are – what are their interests and values? Your child's search history can reveal a lot about their most intimate feelings, hopes and fears. Choose a browser that helps protect them from trackers, and a search engine that doesn't track your search history.

7. Use a VPN

A Virtual Private Network (VPN) can protect your child's Internet use from being observed by your Internet Service Provider (ISP) and bad actors who might be trying to spy on or intercept Internet traffic. If your school district distributes devices, they may already include VPNs. You can research what kind of VPN would be best for you and your child.

Internet Society

© Nyani Quarmyne

8. Regularly update software

Updating software is an easy way to make sure information is as secure as possible. Software updates fix bugs and security vulnerabilities and can make your child's information safer. Run software updates during lunch breaks or after school ends for the day.

9. Backup files

No one wants to have to redo their homework assignment. Encourage your child to save regularly while working on assignments and make a backup in case something goes wrong.

If your child or their school is the victim of an attack, a bad actor can compromise files including important school documents, class notes, and grades – or lock them out. School districts may offer back-up options, but you can also seek out cloud providers and/or external storage devices to ensure that your child's files are safe. Remember to seek out an encrypted and password-protected backup option.

10. Start a digital vault

It's never too early to encourage your child to put together a secure digital vault with important documents and information they may need in the event of a natural disaster, family emergency or other situation. It's also a good place to store copies of after school job references and certificates. Ask your child if they have any memories or files that they don't want to lose (such as graphic novels, stories, photos, videos or art they have created) and put a digital copy in their vault.

11. Request online security training

Suggest your school or library introduces peer online privacy and security training from older students enrolled in computer science, paired with younger students. Not all school districts or libraries will have the resources to offer these services, but someone within the community may know someone who could help find the human and financial resources to do this.

Internet Society