11 Ways to Teach Children Internet Safety Best Practices

Going back to school is an exciting time of the year, but it also means children will be using the Internet on a regular basis at school and at home to complete school assignments. That means teaching children **internet safety** and giving students **cybersecurity** tips is especially important at this time of year.

Children's' lack of basic knowledge about online privacy and security can very easily lead to identity theft, downloads of malicious files, exploitation and so on. Another danger is cyber thieves, who see easy targets in children. Cyber criminals, for example, can combine a child's Social Security Number with a fake date of birth and address to open bank accounts, get credit cards or loans.

Please take a look at some tips & tricks parents and teachers can implement to teach children about Internet safety and cybersecurity.

The Ultimate Guide to Student Internet Safety at School: Part 1

1. ***Lay out some ground rules****.* Whether a child is a teenager or an elementary school student, you need to give them a few basic guidelines. For example, you can start by telling them that anything shared once on the internet stays there forever and that nothing is 100 percent private.
2. ***Tell them to check with you.*** First, tell children what "personal information" means. Draw up a list for them and tell them clearly that they should always consult with you before sharing certain details with any website or person on the Internet.
3. ***Password protection and usage****.* These days, children start creating their own email accounts at a young age. Although email websites instruct users to choose strong passwords, advise children on what kind of passwords to choose. Tell them that the password could be a mix of characters and special symbols and ask them never to share their passwords with anyone, perhaps even with you. **Diceware**, for instance, is an easy-to-use password methodology, where you roll a six-sided die five times and use the results to pick five random words from the list.
4. ***Curb social media usage****.* Children spend a lot of time on social media, so it's important to let them know what is OK to share and what isn't. Have a talk with your child and discuss the things they should not share on social media, and remind them that everything stays on the Internet forever. If you want to take an extra step in securing your child's online privacy, create fake social media names a and fake school/ city name for them.
5. ***IM and texting.*** Sending messages on IM clients like Messenger or WhatsApp is something every teenager does, but they don't always know that their chats are not 100 percent private. Therefore, you should advise

them never to share personal data, banking details or other sensitive information like passwords via messages.

6. ***Share news of personal hacks with them****.* If a child is old enough to understand this, share the latest news about identity theft or personal hacks with them to make them aware of the dangers they face while using the Internet.
7. ***Explain the dangers of free public Wi-Fi****.* Kids love free Wi-Fi – who doesn't? Cafes, shops, and even school cafeterias might have unsecured Wi-Fi networks. Explain to your kids to be especially cautious when connecting to these networks – as they can easily be monitored. One of the best ways to safely use public Wi-Fi is by installing a VPN. You can pre-install a VPN on a mobile device and teach kids to turn it on whenever using public Wi-Fi.
8. ***Use a VPN****.* For ultimate protection, install a VPN service on the device they use to encrypt their online communication data. A VPN, or Virtual Private Network, creates a connection tunnel that automatically encrypts all the data coming in and out of your device and effectively protects anyone using the Internet. .
9. ***Warn them of game scams.*** Agree to install games together with your kids. Research to see if the game and the provider are reputable. Make sure you download the games only from a reputable source after reading some reviews. Too often fake games are uploaded online, which are made to pop with color on websites, prompting kids to install them for free, when in fact it's malware that could infect your device.
10. ***Communication with strangers.*** The Internet is as social as ever. New chat rooms (often within video games) and forums uniting different interest groups are popping up every day. As kids are eager to discuss their interests with peers, it is important to speak to them about sharing one's private information. Under no circumstances should they share any pictures, addresses, etc.
11. ***Email deals are fake!*** All that sparkles is not gold. If your kids receive an email about a great offer like a free cell phone or concert tickets – it's a trick designed to get one to give up personal information. Again, advise your kids to always show you such emails and never respond to them.