INTERNET SAFETY FOR KIDS

Kids today have it better than we did as children. Whereas we had one (if we were lucky) channel to tune into on the TV, they have about a dozen. Whereas we didn't really even have much available to us on the internet, there is absolutely no shortage of information at all out there for them to consume, enjoy, and appreciate. There are videos, games, social networks, movies, and it would take many lifetimes to enjoy them all. But with these opportunities comes an opportunity for others to exploit our enjoyment, as children don't have their guards down like more savvy tech users do, which means they're at risk to be targeted to cyberattacks, phishing attempts, or whatever else a hacker would be interested in exploiting a child for. Internet safety may not have been a consideration to us when we were children; now, we think it should be taught in schools.

But since it's not, we're here to give you Internet Safety for Kids 101 below:

1. Posting Online

Children and teens often don't understand that if they post something online, it will likely remain there forever – or until the internet collapses. The simple fact is that the web has no "delete" button, so anything you post on it will remain there. Sure, an embarrassing post, photo, or video can be deleted, but if someone manages to screenshot it or save it before it's done, there's nothing that can be done about it.

Young children and teens will obviously not think about what a future employer or spouse might think about what they post on the iInternet under their real name. Such lack of foresight can – and likely will – eventually come to bite them in the future. Plus, they might post the kind of information (like their current whereabouts) that can make it easy for criminals to target them.

2. Malware and Viruses

Kids and teens can download malware and viruses by accident without even being aware of it. The malicious files can be disguised as the latest video game, their favorite singer's album, or sexually explicit photos and other content. Youngsters don't normally consider the possibility that such a file could contain anything malicious, so they don't think there could be any consequences if they interact with them.

Because of that, their devices – and, consequently, your devices if they use them – can end up infected with all sorts of malware like spyware, keyloggers, and adware. If that happens, rest assured your and your kids' personal and financial information will be stolen and sold on the deep web. That won't be good for any of you.

3. Cyberbullying

If you’re not familiar with cyberbullying, it’s when people use online and electronic communications to threaten, intimidate, and scare kids and teens. They can target older people too, but kids and teens tend to be the main victims

How can you improve internet security for kids?

Install Secure Antivirus

You should discuss malware with your kids: what it is, how their devices can be infected with it, and what kind of damage it can do. To avoid such situations and guarantee internet safety for kids, it’s best to install antivirus/antimalware software on all your and their devices. Don’t be fooled by the name – both antivirus and antimalware programs do the same thing. A virus is a type of malware, after all.

Installing VPN on their devices

A VPN, or Virtual Private Network, is a technology used to add privacy and security over the internet by hiding your real IP address and encrypting your traffic. VPNs also enable you to access the internet freely and anonymously without having to worry about surveillance or censorship.

A VPN service would encrypt the users’ internet traffic, which can come in handy when they use public Wi-Fi. The majority of the kids (and adults, quite frankly) use public WiFiwithout caring that it is unsafe and that anybody could monitor their online activities. What they don’t realize is that this carefree attitude pretty much means a cybercriminal could easily steal their email, social media account, and bank account login credentials without them even knowing.

Another way a VPN would help secure internet safety for kids is by hiding their IP addresses. Why’s that important? Because their geo-locations will be hidden this way, so shady websites and hackers won’t be able to monitor that kind of information. In other words: they won’t know where you live. (But without a VPN, they will!)

Better Gaming Experience for your kids: Your kids would no longer have to worry about region restrictions, IP bans, DoS/DDoS attacks, games being banned, and high ping times and lag. Plus, it’d let them play some new games earlier, especially if you reside in a country that releases games later.

Avoid Geo-restrictions: VPNs work to avoid geo restrictions applied on websites, which means that you and your children can watch the shows, cartoons, and movies you want.

CONCLUSION

Internet accessibility is important nowadays for everyone including teens. The Internet can help

them do their homework, gaining some knowledge and of course playing games in the free time. But, As parents, it is our responsibility to make sure that our children are safe while using the internet.

Here is a list of our recommendations that you can try to make sure your kids are safe when using the internet.

- Use Antivirus
- Use VPN
- Use children friendly browsers
- Tell them about Phishing attempts
- Discuss cyberbullying with them.
- Do use parental control on the devices

Was this article helpful? Rate and share your comments below. Your input matters to us and everyone else in the Cyber Security Community.