HERO
IT SUPPORT

Internet Safety Tips for Parents 2019

Internet Usage

1. Keep the computer in a common area of your home

2. Set rules and guidelines and discuss why these are important

3. Under GDPR, protecting the personal data of children is a priority. Companies are not authorised to gather personal information from children under 16 without asking for consent from a parent or guardian. Talk to your child about this and the importance of not using a fake birthday or age in order to set up any account online

4. Encourage children to use strong passwords, to not store them anywhere and to never share them with anyone

5. Express how important it is for children to never click on any links from unknown contacts in emails, texts, websites, social media or online chats

6. If your child is online shopping, you need to explain how card details can be stolen. If providing your child with a card to pay online, consider give them a credit card, as this is easier to solve fraud with than your bank card. Also make sure they never save your card details online

7. Never let your child download anything without your permission. Downloading content can sometimes end up in your computer being infected with Malware and Viruses. You can set your child account so it doesn't have admin permissions, therefore they would require a password every time they wanted to download content

Emails

1. Educate your child on what a suspicious email looks like

2. Stress how they should never open an email from an unknown contact or banking, credit card or financial companies

3. Teach your children to ask before clicking on a link in an email so you can check the authenticity of the link prior

4. Ensure your antivirus is up to date and if you have a firewall, the security settings are fully configured

5. Take a look at Google's 'Family Link' to create and control child email accounts and their devices. Other brands have similar versions such as Apple 'Families'

Social Media

1. Age restrictions are in place for a reason. The age restriction for Facebook, Snapchat, Twitter, Instagram, Musical.ly and Skype is 13. However, WhatsApp raised their age limit to 16 last year. There is no age restriction for watching videos on YouTube, but to have a YouTube account and upload videos, users have to be 13

2. If your children do use social media, make sure you are friends or connected, depending on the social media platform. Being able to view their full profile gives you an idea of the public information your child is providing

3. Some social media platforms now have locations enabled, meaning people who are connected with your child on that social media can rack exactly where they are. The two main ones are Facebook and Snapchat. You can turn these off and should. Children should also bare in mind when they post to a location, that everyone will know where they took the photo, so it is best not to add locations to images relating to school and home to prevent people finding out where your child can be found

4. Set up privacy settings on your child's social accounts to ensure they are using social media securely with little information revealed

5. Encourage your children to only accept friends and followers online who they actually know and to keep their profiles private so people have to request to follow your child's account. This way they have control over who is following them

6. Make sure your child uses nicknames and never reveals any personal information such as age, location or gender

7. Never allow your child to meet with someone they have met online. If you do allow them, go along with them

Mobile Phones

1. Set up emergency contact details and medical details on your child's phone. If an emergency ever happened and your child was not under your supervision, whoever is caring for your child can access their emergency contacts and medical information without having to unlock their phone. This could save their life, especially if they have life threatening allergies. It is also a good idea to teach your children how to access your emergency contacts on your mobile device

2. Enable GPS location tracking and share with yourself only. This way, if you are concerned about where your child is and you are unable to contact them, you can see where they are. This is also a good idea if the phone becomes lost or stolen, as you can track where it has gone

3. Disable location settings for all other apps to ensure no one else can track your child

4. For extra security, you can download an app such as 'My Mobile Watchdog'. This parental control system allows you to see every activity on your child's phone

5. Set a good example when using mobile phones. Don't use yours whilst driving or at the dinner table

Final Tips

It is important to talk to your child about internet safety and why you are setting up their devices. They need to trust that you are not spying on them but that there are real dangers and consequences involved with the digital world. Guidelines, or rules need to be set and tell your children that the settings have been optimised to maintain their security. Discuss the fact that people aren't always who they say they are online.

Remind your children that the mobile phone, tablet, computer and WiFi is owned and paid for by you. Rules and guidelines must be respected and observed, including screen-time.

Ensure your antivirus is up to date along with your firewall, if you have one, in case a malicious link is clicked.

Finally, teach your children about online reputation. Understanding this at a young age can make a huge difference when they grow up. Many children don't know the impact social media can have and that everything that is posted is permanent, even once deleted. Explain what their digital footprint is and how inappropriate images and messages can impact their future when it comes to employment.

Always remember....

What goes online, stays online