CYBER AWARENESS FOR PARENTS

Home is a place that gives a sense of security and safety. To ensure digitally safe and healthy environment at home, certain practices need to be followed-

1. Digital Devices Under Parental Supervision: Parents can help younger or older children to explore online, as well as help them to manage their accounts and compatible devices. Parents can monitor the child's online activity by using apps and setting screen time, etc.

🔋 **Use Digital Device as Family Resource:** Computers and digital devices need to be treated as a common resource for the family. Placing computers in a common area of the house can help for easy monitoring of child's online activity.

- Create a family media use agreement with all family members to encourage proper balance and use of technology.
- Establish limits, routines and guidelines.

🔋 **Set Screen Time:** Set reasonable screen time for any digital device including mobile, TV, computers, gaming consoles, et

🔋 **Apply Parental Controls:** Set parental controls on computers and other devices.

2. Take Steps to Ensure Security: Parents should orient their children about the cybercrimes and data breach which may happen while using the internet.

🔋 **Secure your Wi-Fi:** Wi-fi Check devices connected with home Wi-Fi network and Secure your home Wi-Fi should have a strong password

🔋 **Age Appropriate Use:** Ensure limited access to the websites should depend on the child's age and level of maturity.

🔋 **Turn off the GPS:** Using a simple GPS plug-in may lead to a potential stalker to drag uploaded photos from the Internet and easily read the data connected to the pictures and track the child's location. Therefore avoid publicly sharing your location in your digital devices.

🔋 **Use Bookmarks/Starred Options:** Parents should have easy access to favorite sites and secured sites for their children.

EDUCATING YOUR CHILD

In a world where children grew up along with digital devices which play an integral role in their life, it is important for parents to play an important role in teaching and helping them to learn healthy concepts of digital use. Parents may initially provide their support by constantly being with them and then retreat, once their children have practiced and gained confidence. Here are some ways in which parents can teach children about online safety need to be smarter to help their child navigate this world with the appropriate skills, behaviours and thinking, to become not only safe but also happy and resilient users of digital technologies.

Enable them to be **'SMART'** when they are online with the following aspects:

S- Stay Safe - Never share personal information to anyone

M- Meetup - Never meet with anyone you do not know

A- Accepting Files - Never open or download the unknown files, pictures, mails

R- Reliable - Verify the authenticity of the information received before proceeding to act

T- Tell Someone - Inform trusted adult if you see/read something that makes you feel worried/ uncomfortable

🔋 Discover the Internet together with the child and discuss both positive and negative aspects to help them gain the knowledge and develop critical thinking to respond in the right way.

3. Personal Information & Privacy: Children tend to share a lot of personal information online. It is essential for children to understand the hazards of sharing personal information. Parents need to make them aware of many ways to protect personal information and privacy online. It is vital for both parents and children to learn about privacy settings. Awareness is the first step in online safety.

🔋 **Importance of Personal Information:** Make the child understand the importance of personal information and teach them to avoid sharing personally identifying information (e.g., real name, address, school, telephone number, photos, family member names) via the Internet/any online medium. • Sharing Photos & Videos: Discuss the potential problems associated with selfie culture and the possibility that shared images and videos could later be used in exploitative ways.

🔋 **Importance of Passwords:** Educate children not to share passwords, even with their closest friend, and always close their accounts before turning off computers especially in public places.

🔋 **Importance of Financial Information:** Educate them to never share important credit/debit card details and let them know about the dangers and threats of free online offers or fraudulent email claiming huge rewards.

🔋 **Use Privacy Settings Available:** Educate the child about privacy options on various digital devices and social media platforms; Review the privacy settings for posts, apps, and profiles. This way, it can be established which people get to see the child's profile and what they actually see; and to set the security features of browsers to "high".

4. Pitfalls of Social Media & Safety Measures: Social media connectivity presents positive opportunities and benefits as children use to chat with friends, network socially, share photos, make music videos, upload videos, play games, visit chat rooms, use file sharing sites, etc.. At the same time, children may encounter the following online risks while using social media:

🔋 **Online Chatting:** Keep the youngsters away from online chats and try to apply the old rule, "never talk to strangers". Also discuss the dangers of meeting the person they befriend online without permission.

🔋 **Online Grooming:** Educate children about online grooming and the hidden dangers from strangers trying to win child's trust with wrong intentions.

🔋 **Cyberbullying:** Discuss with children about cyberbullying and make them well aware that online harassment can cause grave emotional issues, therefore they should seek immediate help when required.

5. Teach about the Darker Side of the Internet: Internet is a great source of information for children, but they need to be aware about the hidden dangers of using it.

Need to Fact Check: Teach the child about the huge amount of information available online and the possible ways to evaluate the authenticity of such information.

🔋 **Avoid Unauthorised Websites:** Educate them to never visit unauthorized websites or sign up for every website. Many social networking sites (YouTube, Instagram, etc.) have age restrictions.

🔋 **Malicious Links:** Inform children about the malicious links on video sharing sites like Youtube, Instagram, and alert them to avoid clicking on such links which offer exciting benefits.

🔋 **Fake Profiles:** Educate the children about the celebrity chat groups/pages. They should be made aware that these celebrity social media accounts /pages may not be running by the celebrities or their fans, and they need to be cautious about it.

ENABLING SECURITY FEATURES FOR DIGITAL SAFETY

It is important that the parents are digitally aware and up to date to implement and enable some important security features and practices when they are online or are using the digital devices.

Basic Security Measures:

🔋 **Ensure that all operating systems installed in your device are updated with the latest security updates as soon as they come out.**

🔋 **Do not install any software without reading the license agreement and make sure your children ask for your permission before downloading or installing something on your devices.**

🔋 **Do not do online transactions on websites without 's' in their URLs https://. "S" in "https" stands for "secure"**

🔋 **Do not share your financial details like credit/debit card/UPI on educational websites or gaming sites. Disable purchase options to avoid any unknown account charges.**

Smart Ways for Digital Parenting:

🔋 **Check with your Internet Service Provider for any parental controls, tools they may offer.**

🔋 **Use filtering options for your child on browsers to avoid unnecessary websites with inappropriate content.**

🔋 **Parents should ensure that they do not leave their devices unattended as children might explore or misuse the device.**

🔋 **Discourage your child from downloading games and other media which could harm programs on systems by unauthorized users.**