09 Apr 2020

MINISTRY OF DEFENCE
CYBER CELL

CYBER SECURITY ADVISORY 05/2020: ONLINE SAFETY OF CHILDREN AND PARENTS

1. In the prevalent lockdown scenario most personnel of MoD have been encouraged to work from home. The Internet is good resource for children to prepare school reports, communicate with teachers / other kids and play interactive games. But online access also comes with risks, like inappropriate content, cyber bullying, and online predators. Using applications and websites, attackers may pose as a child or teen looking to make new friends. They may entice the child to exchange personal information, such as address and phone number, or encourage kids to call them. Parents should be aware of what their kids see and hear on the Internet, who they meet, and what they share about themselves.

2. In this scenario, the following cyber security best practices are strongly recommended for children / students:

(a) Think carefully before posting pictures or videos of yourself.

(b) Once you've put a picture of yourself online most people can see it and may be able to download it, **it's not just yours anymore**.

(c) Never reveal personal information, such as address, phone number, or school name or location.

(d) Use only a screen name and don't share passwords (other than with parents).

(e) Never respond to a threatening email, message, post, or text.

(f) In case of doubt, cross check with the sender (friend / school / other source) on the authenticity of the doubtful communication.

(g) Always tell a parent or other trusted adult about any communication or conversation that was scary or hurtful.

3. The following cyber security best practices are strongly recommended for parents:

(a) Set a rule that the child should use the electronic device for browsing in the living room or in the presence of an adult. Keep devices in a common area, by locating all computers, TV and devices in a common area, parents can easily ensure that the child does not view unsuitable content online, and also supervise the child's online activities.

(b) Consider two-factor authentication for devices and lock the device's home screens with a PIN.

(c) Online communities are here to stay, so consider starting social network safety talks early. Several kid-friendly browsers, apps, and social networks exist online for younger kids and are perfect for teaching them about privacy settings, how to collaborate and interact with others online.

(d) Spend time online together to teach your kids appropriate online behaviour. Going online with your child gives you the opportunity to see the apps or games your child plays, or the videos he / she watches.

(e) Filter content. To avoid the chance of your child encountering inappropriate content by mistake, consider adding parental control software to family devices.

(f) Talk about the sites and apps teens use and their online experiences. Discuss the dangers of interacting with strangers online and remind them that people online don't always tell the truth.

(g) Teach the kids that the internet provides anonymity and their online friends may not really be who they say they are. Never agree to get together in person with anyone met online without parent approval and/or supervision. Keep track of your kids' online friends and report suspicious activities or people online to your local cyber-crime agencies.

(h) Bookmark kids' favourite sites for easy access.

(j) Find out what, if any, online protection is offered by your child's school, after-school centre, friends' homes, or any place where children could use a computer without your supervision.

(k) Take your child seriously if he or she reports an uncomfortable online exchange. Report the matter to cyber crime authorities if needed.

(l) Check your credit card and phone bills for unfamiliar account charges.

4. These guidelines may be disseminated to all concerned agencies within the MoD.

Reference: CERT-In Advisory CIAD-2020-0012