Dr. Prabhu addresses India's Largest Online Parenting Summit 2021 on Cyber Security

Here are the excerpts of Dr. Prabhu's answers to the questions posed in the panel discussion.

Question 1

The connectivity of IOT devices carries an inherent risk of unknown third parties gaining access to your personal data. Ananth, what can happen if our connected devices are not secure? When can protecting our children become an invasion of privacy?

This is a very important question. Before I answer that, Let me Explain what a Smart Object or a connected object is! Any tangible object (that we can touch) + Processor+Sensors+internet becomes a Smart Object! Earlier, we had a regular AC. Now we have SMART AC! You talk to it using an app on your smartphone, wherever you are- either control the temperature, switch it on or off, check usage statistics or even set geo fencing so that it automatically switches on when you are 1 km away from reaching home, after a tiring day at the office.

The Internet of things (IoT) emerged as a concept about 20 years ago and is now making headlines around the world. Everyone talks about connectivity, smart devices, real-time data extraction, data security, privacy!etc

In the last year, Cisco estimated the year 2020 would see 27 billion devices added which is 4 times the human population, while (Security Today) estimated it would be 31 billion new devices. Either way, that's almost 1000 new devices each second! The number of connected devices in 2021 is set to hit 46 billion. (Source: Juniper Research). Oh yes, after the pandemic, everythings went online! Smart consumer electronics fall into this category.

Technology is a double edged sword. There are advantages and disadvantages and we should know how to use it responsibly to make our lives better. However, the proliferation of all these devices in our everyday lives also poses security risks as you have rightly asked this question, unless secured properly. These devices can be used as new avenues of attack by cybercriminals. Hackers sitting anywhere in the world can easily breach a smart device and spy on the owners if those devices are not secured properly. They can get into industrial control systems, manipulate production lines, shut down factories, we have recently heard about the gas pipeline attack in the US of A, and even cause shipwrecks. We have also heard tales of couples breaking up because they figured out their partner was cheating on them by the activities on the dashboard of their fitness trackers. Well, A simple hack can turn your child's smart toy into a spying device.

Having said that, We cannot avoid the technological revolution. Connectivity brings far too many benefits to neglect especially for the parents to keep track of their children- with devices like Home CCTV Cameras, geo fencing watches, activity trackers and many more. Therefore, it will soon become something as natural as electricity or tap water. Earlier it was Roti Kapda Aur Makaan! Now it's Roti Kapda Makaan Aur Internet, woh bhi 4 G. And soon, we will all be upgraded to 5G.

IoT security needs coordinated efforts and holistic approaches by all stakeholders, from manufacturers to end-users. "If you connect it, protect it." should be the mantra. Unicef has an exclusive Innocenti Research Center that works on Global Challenges and strategies for Child Safety Online!

Well, we can surely protect ourselves as well as our smart devices. It all begins with securing the Wifi Routers- by using strong encryption methods, Encrypting

your web traffic using VPN to avoid man in the middle attacks so that nothing comes in between u and your smart device!Besides shielding data from prying eyes, it can also allow you to securely access data stored on your home network even if you're a half a world away, and also regularly updating the firmware, using strong passwords.

Coming to the second part of the question, Adolescence is a phase where kids face challenges, and try to understand what they are. It is a phase when a child explores the different social interests and wishes to have a private space where he/she can unveil their true interests. There is a thin boundary between invasion and monitoring. But parents often cross this line and step into activities which they shouldn't be doing. As a parent, you have to protect your children from the hidden (and not-so-hidden) dangers of the world. Now that your pre-teens and teens have access to smart devices, they're at a higher risk of being exposed to life's harsh realities. Without proper supervision, a smartphone or tablet can allow your children to connect with strangers, learn obscene behaviors, and engage in other horrendous acts. We have also seen instances where parents use apps like Google Family link, mSpy, Hoverwatch, Flexispy and others to monitor activities. However, this doesn't mean you have to restrict your child from smartphones and connected devices. Instead, you can monitor and limit their activities. You'll thank yourself later when you stop your child from getting into a heap of trouble.

But when we talk about the larger picture, An important children's privacy law in the U.S. is the Children's Online Privacy Protection Act (COPPA).Well, The Indian government introduced the Personal Data Protection Bill, 2019, in the Lok Sabha on December 11, 2019, and it has subsequently been sent for review to a joint parliamentary committee. Under Chapter IV, Section 16 of the bill deals with

personal and sensitive personal data of children.

--

Question 2

According to a recent social media poll by Godrej Security Solutions, 78% respondents said that their video data is safe with home cameras, and 79% respondents said that their data is stored on a memory card. Ananth - what are your views on this? Also what should one keep in mind when installing new devices at home?

I would like to quote IP Camera as an example and answer this question.

Network or internet cameras — usually marketed as IP cameras — are popular for keeping an eye on your property, your family, and your pets. These cameras provide live video and audio feeds that you can access remotely using an internet browser as the data is stored in the cloud.

When you want to buy a Home security camera, there are 5 features that are most important from the Video Quality, Motion Sensing, Low Light Output, 2 way audio, recording and storage.

So there are 3 concerns,

1. Can someone Hack into the IP Camera and snoop on us
2. Will the hacker be able to sniff the packets sent from camera to cloud to intercept the messages
3. What about Stealing data from the cloud?

Although many manufacturers include features such as night vision and motion detection in their IP security cameras, many of them do not actually have real concerns about things like secure streaming. Simply put, you could be hosting the world's biggest open house! Most IP cameras use the default password, and you do not need to change the default password during the setup process. That is how

Shodan and Insec camera websites live stream cameras across the world. In addition, these passwords are so weak that hackers can easily sniff them out. It is also common for cameras to show users' Wi-Fi passwords, email addresses, and FTP access settings once the hacker takes control of it.

Now the bigger question is, how is data secured! Am glad, Godrej has always been a name that resonates with trust and their cameras are robust!! Servers of Godrej are in India! Unlike the chinese cameras which are available in the market with servers stationed in china or some other country because you do not know what they do with your data! Remember, Data is the new oil!

The first line of defense to accomplish this is to deploy IP devices and system components with encryption solutions such as the proven 256-bit Advanced Encryption Standard (AES) which the Godrej uses to scramble and unscramble the data. To date, there have not been any confirmed hacks of AES 256 encrypted systems with the exception of faulty implementations. This actually tells how secure the data is!

Once you've bought your IP camera Keep the software up-to-date, Use a strong password, Enable https instead of http. Before you access your camera from a phone or mobile device, Confirm that your app is up-to-date, Password-protect your phone or mobile device, Use a secure Wi-Fi connection. It's also a good idea to change the settings on your mobile device so that it doesn't automatically connect to nearby Wi-Fi.

I am glad, all the participants will be getting a copy of the revised Cyber Safe Girl v4.0, Beti Bachao Cyber Crime Se, yes Cyber Crime is gender neutral, but this project was inspired by Modi jis vision of Beti Bachao Beti Padhao. The book

comprises 40 new gen cyber crimes, that also includes about Smart Homes and one bonus chapter on CCTV at home.