UN/ITU Webinar on "Online Safety and Security during COVID19" – 6th May 2020

What is the scale of the cyber threat and, amid COVID19, how could government more actively address the threats to secure the society?

Warm greetings to all of you from the Republic of Mauritius.

At the outset, allow me to thank the Office of the UN Under-Secretary-General Fabrizio Hochschild and the International Telecommunication Union for organising this webinar, in these difficult times of the COVID-19 pandemic.

As the crisis around the coronavirus continues to expand, organizations, including governments, are facing unexpected and profound challenges as they seek ways to allow people to stay at home and remain productive.

Since the beginning of the sanitary curfew in Mauritius, we have noticed an increase in bandwidth consumption. Adults are using video conferencing in order to work from home, students are following their classes online and, of course, there are a lot of avid fans of Netflix or Youtube in Mauritius.

Fortunately, this 50% increase in bandwidth has not had any negative impact on the quality of service as our national network has been built with robustness and performance in mind.

As this shift is occurring, cybercriminals are developing tactics to take advantage of those who have inadequate security equipment or procedures.

This is a big and important challenge to overcome.

Of course, there is a technical aspect, which includes the use of Virtual Private Network connections, encryption, the use of firewalls, etc.

But you will all agree that, in many cases, the human element is the most fallible. As such, it is important to have comprehensive measures to educate our citizens on how to respond to cyberthreats.

In Mauritius, we have observed a change in the pattern of cyberthreats during this lockdown period as compared to previous months.

Statistics gathered from the Mauritian Cybercrime Online Reporting System reveal the following:

- We have witnessed an increase in scams by a factor of 2 and a ½ as compared to February. Examples of scam include extortion emails, lottery & charity scams, fake online shops and various fraud schemes.

- Similarly, fake media accounts spreading fake news have increased by the same factor over the month.

- Hacking attempts are now twice as prevalent as in February.

Because of these alarming statistics, the Government of Mauritius has taken a number of measures to make the Internet more secure while allowing our citizens to work from home. Some of those measures are:

- The Mauritian Cybercrime Online Reporting System which is an online platform for citizens to report cyber-incidents as soon as they happen for the appropriate authority whether it is the police, the Computer Emergency Response Team, the Data Protection Office or the ICT Regulator.

- The Computer Emergency Response Team of Mauritius also issues security alerts, guidelines and best practices on a regular basis. A dedicated section has been created and has issued a guide on how to securing a remote workforce in the time of COVID-19.

- A Security Operations Centre is being setup within the datacenter of Government to monitor cyberthreats in real time and prevent cyberattacks.

- We are also carrying out sensitisation campaigns on radio and national TV to inform citizens about current cyber threats and how to react to them.

- And, of course, we are also looking at strengthening our legislation concerning cyberthreats and cybersecurity.

Of course, this is just the beginning for us. Mauritius is a small island in the middle of the Indian Ocean and it is essential for us to be inspired by cybersecurity measures that other countries have put in place.

This is why I am very happy to form part of this high-level seminar today. My intention is to listen and learn from all of you.

I strongly believe that the international community should unite together to fight the cybersecurity challenges posed by COVID-19.

Thank you for your attention.