Cyber Crime Trend & Digital Safety amidst COVID-19 Pandemic

Hackers have been increasingly cashing in on the global Coronavirus pandemic by spreading malware through emails, websites and apps designed to look like Covid-19 related resources. India has witnessed a staggering 86% surge in cybercrimes and phishing attacks over the last 15 days. These include all kinds of cybercrimes and are not just limited to financial fraud or data breaches.

Furthermore, according to the UN Special Rapporteur[1], women suffer serious consequences as they are disproportionately targeted by online violence. Cyber Violence has real consequences and costs. It undermines women's wellbeing, their rights, and their progress in all aspects of life. Cyber violence results in psychological, physical, sexual or economic harm to women.

Given the increase in digital interactions due to the pre-cautionary measures put in place in India (and many other countries around the world), many children and women are being encouraged to use digital technologies for the purposes of education and work, amongst others. Many of these users could be first-time users and/or may have a limited understanding of good practices when interacting with others in cyberspace. Creating awareness, and clearly communicating what the best practices are, will be key to inculcating good and safe cyber-habits.

In these times, criminals have used popular apps like Zoom, House Party and corona trackers to build the trust with their targets, whether male or female, to conduct such attacks.

According to a Checkpoint report, there has been nearly 50% surge in the number of coronavirus-related domain names registered in the past couple of months. The report

[1] Human Rights Council (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. A/HRC/38/47.

states that there were over 4,000 coronavirus-related domains registered globally and these domains are 50% more likely to be malicious. Needless to say, that hackers are trying to use the present scenario to their advantage and netizens need to be extra careful while searching for content on coronavirus. It is obvious that many of those malicious sites will be used in phishing campaigns. Phishing emails are the ones that appear to be from a trusted source, tricking users into providing sensitive information, downloading malware, or clicking a link to a website that can do either.

India Future Foundation and UN Women invite you for an exclusive session on 'Cyber Crime Trends & Digital Safety amidst COVID-19 Pandemic', from a perspective that ensures a safe, gender responsive and equitable cyber space.

In this session, we will analyze the current situation and capture the changing footprint of cybercrimes:

1. Analysis of Laws and Policies that govern the cyber space.
2. Phishing Attacks, Malicious Apps, Exploits, and Successful Campaigns.
3. Safety Guidelines and Tools - The webinar may delve into the need for spreading awareness on the Do's and Don'ts of cyberspace interaction, with special focus on women and girl's safety.
4. Government Initiatives.