# Cyber Security: Social Engineering at the Time of Social Distancing

## Overview

Cyber world has provided unimaginable power to the individuals. Modern forms of power dynamics have changed, between the state and the actors. Though government has been spending a lot to protect its confidential for the security concerns of the state, individual actors have quite often challenged the efficiency of the state in combating the cybercrimes. Wikileaks would be a good example, which came in International attention in 2010 for the publication of a series of leaks in U.S intelligence, the way individual actors have challenged the power of state.

COVID19 pandemic has brought several challenges for the security of the Cyber. In the backdrop of the lockdown, distance generated in our physical world, majority of people are spending large duration of their time on the cyber world. Since, large amount of time has been spent online, cybercriminals have been using this opportunity to trick people and gather sensitive information. This has led to rise in corona virus phishing and ransom ware hacks along increased online abuse, sexual comments and violence on the women.

There has been continuous rise in social engineering tactic by the hackers to gather security information and get access to sensitive data. Acohido writes, “Social engineering invariably is the first step in cyber-attacks ranging from phishing and ransomware to business emails compromise (BEC) scams and advanced persistent threat (APT) hacks”.

The new ‘social world’, a platform created through internet has come into existence post COVID19 pandemic. The new entrances into virtual social world by quite large section of people have benefitted hackers to carry out their crimes in the time of physical distancing. ‘The Week’ reported that India has witnessed an increase of 2-3 times in cybercrime rates in past few weeks.

The Week wrote, “With almost all the sectors in India practising work from home this has put a humongous strain on the security teams who are responsible for safeguarding backend data and files. The risk is all the higher for the organisation that deal with customer-sensitive data such as banks/NBFCs, healthcare companies, government agencies, etc. Such companies are at the forefront battling these threats,” said Uniken CEO Bimal Gandhi. Even the WHO has admitted that there has been increased cyber threats since pandemic.

## Current Scenario

In today's time, impetus laid on digital-led platforms' have an indispensible role in every individual's life, at varied levels. In the post Covid-19 scenario, the "new normal" invokes the power of extended reality (XR) – an umbrella term encompassing Virtual Reality (VR), Augmented Reality (AR) and Mixed Reality (MR).

Given, there is an increase in the practice of social distancing; the practice of social engineering has seen a subsequent growth in an unprecedented manner. Against this backdrop, it may be rightly stated, how the techniques used for social engineering such as phishing, vishing and baiting inter alia attacks used by people need to be given utmost importance. Having said that, stringent measures pertaining to laws related to cyber safety is indeed, the need of the hour.

## Way Forward

In the case of our country, a symbiotic relationship vis-à-vis social networking and cyber safety and security needs to be emphasized at both levels- national (macro), and individual (micro). In order to attain the same, mitigation of the prevailing pluralistic ignorance towards cyber-led exploitation is required.

The following measures will help in combating the negative externalities of social distancing with respect to social engineering:

- Firstly, an increase in public awareness apropos cyber security (the existing implementation mechanisms, platforms for educating public regarding cyber safety) needs to take place, actively;
- Furthermore, one must always be mindful of every activity that takes place at a virtual/digital level in order to combat the risk of cyber crime;
- Post recognition of activities related to cybercrime, the process of easing out prevention of the malpractices will in turn ease out the way forward. In addition, continuation of stringent measures vis-a-vis implementation mechanisms on behalf of the government will aid in attaining the said objective.