Piercing the veil of anonymity: Remedies and challenges in curbing technical support scams

Thought Leadership • April 30, 2021

This article was first published in the 30th April 2021 edition of the Asia IP magazine.

Author: Saif Khan, Deepank Singhal

With the advent of technological advancements and an energetic young English-speaking workforce, India has established itself as the most sought after destination for leading IT companies and business process outsourcing (BPO) industries globally. These industries have been constantly contributing towards the generation of revenue and employment opportunities while providing a significant boost to the Indian economy in recent years.

However, this global repute of India of being a hub for IT and IT-enabled (ITeS) services is in serious jeopardy with increasing instances of technical support scams originating from fake call centres in various parts of India. These call centres carry out illicit activities to dupe innocent consumers on the false pretext of providing technical support services. In this New Age world of crimes, where the criminals have transcended from the streets to our computers and telephones, instances of criminal acts in cyberspace are at its peak, as according to the *National Crime Records Bureau (NCRB) Crime Report of 2019*, cyber crimes in India have jumped over 63.5 percent in comparison to 2018 with 26,891 out of 44,546 cases registered for motive of fraud.

As recently as in March 2021, the Delhi Police's Cyber Crime Unit (CyPAD) arrested 34 people in a raid on two fake call centres in Delhi for allegedly impersonating Apple and McAfee employees and defrauding 8,000 victims in the United Kingdom, Canada and the United States of more than US$1.38 million. In another investigation in October 2020, the Central Bureau of Investigation (CBI) seized assets worth around US$25.2 million during a search and seizure operation on six companies accused of running technical support scamstargeting Microsoft customers in Delhi and the National Capital Region. The investigation was conducted in collaboration with law enforcement agencies from the United States. In October 2018, the Cyber Crime Cell in Delhi arrested 24 people in search and seizure operations on 10 such fake call centres engaged in technical support scams in a complaint filed by Microsoft India. Similarly, a month thereafter, 42 people were arrested from 17 fake call centres in Noida and Gurugram for impersonating Microsoft employees and swindling innocent people. Indian law enforcement agencies have investigated several such entities in past 10 years; judicial proceedings are also pending in Indian courts against such entities for defrauding vulnerable individuals on the false pretext of providing technical support services to repair their personal computer systems in addition to infringing upon the valuable intellectual property rights of the IT companies.

Hiding behind the veil of anonymity, these perpetrators approach victims using various methods including making unsolicited calls, unsolicited dubious links re-directing to deceptively similar webpages of IT companies; internet search engine advertising through key words like 'technical support service' for major IT companies like Microsoft, McAfee, Norton, HP and others; web browser pop-up messages indicating malware infections or other computer errors in the victims' computers; etc. These perpetrators hold themselves out to be certified technicians of the reputed IT companies, deceiving consumers into believing that their personal computers and software are infected with dangerous viruses and malwares, which, if not attended to promptly, will lead to permanent damage to the computer system. Thereafter, they will sell unwanted services to purportedly clean the victims' systems while actually installing infringing or otherwise illegal copies of software.

Investigations by law enforcement agencies have revealed that, typically, victims of these scams permit these fake technicians access to their computers; the fake technicians then falsely identify various computer files as malware when the files are, in fact, benign. Additionally, these fake technicians sometimes even load malware on victims' computers and steal sensitive information and data files while pretending to fix non-existent computer viruses.

The ambit of the offences committed by such perpetrators is significantly wider, which includes unauthorized access to a computer with an intent to cause damage to the system, stealing sensitive information, cheating by impersonation, extortion, forgery, money laundering, trademark infringement, copyright infringement, unfair competition etc., attracting provisions of various laws including the Information Technology Act, 2000; the Indian Penal Code, 1860; the Prevention of Money Laundering Act, 2002; the Trademarks Act, 1999; the Copyright Act, 1957; etc.

Remedies against such acts of these fraudulent entities/individuals are available to the victims as well as the company which is being impersonated by such entities both under criminal and civil law. They may file a criminal complaint under the relevant provisions of the IT Act, Penal Code, PMLA, etc., and additionally, the company may also initiate a civil action by filing suits for injunctive relief and damages for contractual breaches, infringement of trademark and copyright, and unfair competition.

Untraceability of the master minds behind such acts and attributing the said crimes to these individuals remains the biggest challenge for law enforcement agencies as it was further discovered during the investigations that the operations of these entities are not restricted to targeting victims merely in India but that they often operate in collusion with similar fraudulent entities based in other countries in order to target victims globally. This further enables these criminals to commit tax evasion by opening an offshore account in the name of foreign entity to channel their illegal money.

In order to curb the menace of technical support scams and achieve the ultimate objective of making the cyber space safer for consumers, the need of the hour is close cooperation between law enforcement agencies across the world through mutual legal assistance treaties and IT companies

for spearheading the consumer awareness campaigns against such scams.