Food and Scientific Reports
ISSN 2582-5437

Impact of Lockdown on Increasing Rates of Cyber Crime

Sanchita Naha*, Md. Ashraful Haque

Scientist, ICAR-Indian Agricultural Statistics Research Institute, New Delhi 110012, India

ABSTRACT

The entire country is exposed to an unprecedented viral infection, where staying at home and social distancing became the only solution to control the spread of the virus. While, majority of the people are trying to maintain the norms, they are compelled to use Internet for conducting day to day activities. Internet not only helped the crowd to cope up with the difficult situation, but it also opened new doors for several cyber fraudsters to conduct criminal activities. A significant amount of increase in the rate of Cyber crimes have been observed during the phase of lockdown. This article provides a better understanding of different kinds of Cybercrimes, reported cases and measures to tackle them.

On 24th March, the honourable PM of India declared a nationwide lockdown for 21 days (later extended) as a preventive measure to COVID-19 pandemic. The lockdown enforces no public movement and social gatherings across the country. All public transports, educational and research institutes shall remain closed except only essential services like grocery, medical stores, banks, hospitals, police forces and power generation units etc. were allowed to function normally.

As an effect of lockdown people were staying at home and practising social distancing to curb the spread of the virus. This has lead to spending most of their time on social media platforms, watching online movies, web series, reality shows on several online entertainment platforms such as Netflix, Prime Video, Hotstar, YouTube etc. Commercial as well as private establishments were continuing their services by allowing their staff to work from home. These companies were conducting conferences, meetings, seminars, discussions through different video conferencing apps like Zoom, Microsoft teams, Skype etc. Schools, colleges and research institutes also started relying on online platforms for conducting classes. Consumers also preferred e-stores instead of going to markets for buying essential goods. This huge usage of the social media platforms, online entertainment and video conferencing apps has resulted in a steep increase in the rate of internet traffic.

While technology came at rescue in this huge crisis, it created several new criminal opportunities as well. Computer and smartphones turning into the focal point of education, commerce, governance and entertainment, it also became the most vulnerable point for carrying out several illegal activities. Cyber fraudsters were clearly having a field day and resultantly, the number of cyber-crimes also showed an increasing trend.

Understanding cyber-crimes: Cybercrime typically refers to a group of criminal activity, being committed by using digital communication and information technology. It includes identity stealing, privacy violation, money heist, fraudulence, and stealing intellectual property rights using a computer as the central device, also known as computer-crime. Generally it falls into two categories. One is where an organization's network or an individual's device is attacked with a virus, malware or DOS (Denial of Service) attack while in the other one the victim is tricked by sending phishing emails, cyber stalking or by stealing his/ her personal information. The difference between crimes in general and cybercrimes is the use of Internet in the later and the attack on an individual's virtual identity. In today's digital age, human beings as well as organizations are identified by a bunch of numbers and identifiers stored in several databases. Here the criminal makes use of the anonymity provided by the Internet to cause harm.

One of the most common type of cybercrime includes identity theft. It is the act of acquiring someone's personal information such as name, mobile number, debit/ credit card details and use it for some criminal activity without one's knowledge. Most common identity theft crimes are hacking social media accounts (Facebook, WhatsApp, Twitter handle etc.). The cybercriminals use this stolen information to steal money, access confidential information, participate in a tax or insurance fraud, create fake social media accounts etc. A popular device called skimmer is used inside the debit card console to steal customer's personal information. Another device called shimmer, which is a deep-insert skimmer, has the

capability of reading data even from the chip-based credit/debit cards.

With the increase in the use of smartphones and the consequent rise in the use of mobile phones, banking applications and UPI applications have gained enormous popularity. Hence, the rate of digital transactions have increased. As the services are shifting more towards online platforms, there are high risk of online banking frauds. Cyber criminals can infiltrate the mobile applications with viruses and hack the mobile devices for committing digital banking frauds.

Cyber stalking is another kind of cybercrime in which criminal harasses a person through online messages and emails. They use social media accounts, fake websites and search engines to intimidate a user and instil fear. Usually, the stalker targets the victim with threatening or abusive messages.

Phishing is one of the oldest type of cyber-attack and majority of the cyber-attacks start with phishing campaigns. It involves deceiving people into sharing confidential, sensitive information and money laundering. The most common way of attack is through sending phishing email or messages. The victim receives a malicious mail or text message that imitates a trusted individual or organisation of business such as colleagues, a bank or business partner etc. The word 'phis' is pronounced as 'fish', analogous to fish catching using a bait.

Other cyber-attacks include siphoning and ransomware attacks. Siphoning is to divert the web traffic into fraud or distorted webpages where the hacker intends you to visit not where the user would visit otherwise. So the point of failure in case of siphoning is in the computer network, somewhere between user's request in the search engine and the response provided by the browser. This kind of websites are made usually by illegally copying the content of original websites and ranking those highly using search engine optimization techniques. Ransomware are a kind of computer virus that encrypts data and asks for ransom in return to decrypt the stolen data. Failing to pay the money would cost loss of data.

Cybercrime instances amid lockdown: During the COVID-19 crisis, several new websites were sharing misinformation regarding the preventive measures to be taken, not to spread awareness but to increase the web traffic. Later many of them found to be incorrect when checked with the information provided by WHO. By the time it was verified, it already became viral in social media platforms whose effects could be potentially harmful or dangerous. Around 4000 fraud portals have been created across the globe by cybercriminals to siphon off the monetary help provided in several government organisations. On 16th of April, Google reported about 18 million daily malware and phishing emails related to COVID-19 scams just in a week. This was in addition to the 240 million daily spam messages related to coronavirus.

Since lockdown, 160 cases of cybercrimes have been reported in Hyderabad. On 14th April itself, registering 7 cases in a single day. On the same day a fraudster siphoned off Rs. 92000 from a private farm employee's bank account promising him to deliver a bottle of brandy. Two Hyderabad men was tricked into a total amount of Rs. 1.2 lakh by cyber fraudsters. One of them was asked to update his Paytm KYC and shared his OTP in the process. Another army official was trying to buy an already owned car through a popular online market portals and contacted the concerned person through telephone. The fraudster asked for 60000 advance cash, the customer gave the money and never got the car in return. These fraudsters took advantage of the obligation of customers to use digital platforms for communication and as well as trading.

A retired government employee from Habsiguda, Hyderabad was waiting for a courier service. He searched Internet for customer care number and a fraudster posing as an employee made him fill his debit and credit cards using Google form sent through SMS. The victim lost Rs. 90000 in the process.

In the 3rd week of lockdown, Maharashtra also reported a 25% increase in cyber-crime incidences. Even big companies fall prey to cyber frauds in the middle of the pandemic.

The tech solution provider Cognizant generating a revenue of more than $15 billion was conducting business with 90% of their employees working from home during the phase of lockdown. In the midst of this, on 25th of April the company confirmed being hit by 'Maze' ransomware. This virus spreads over the network encrypting all the system's data in its trajectory. Once attacked by the virus there's no way of looking back apart from paying the ransom. No backup and recovery system would work because the virus makes a copy of the data stolen and exposes it to the attackers. Even if the company pays for the ransom money,

they have already lost a portion of their customer's data which is vulnerable in any attacker's hand if they have the scope to monetize it. This kind of a cyber-attack apart from causing monetary loss would cost a lot on the reputation of the company. It would be hard to gain customer's trust on the security claims made by the company.

Video conferencing app Zoom recently garnered enormous popularity with 200 million daily active users. But very soon user's started to post online complaints of bombing video meetings by strangers and leakage of confidential meeting recordings on the web. For the application failing to provide security to the users, it was declared unsafe for use by Indian governments as well as companies like Google, Apple, NASA and Tesla. All these organizations released advisories for safer conduct of video meetings using the app. Several video footage of zoom online meetings became available on the Internet putting the organizations private data at risk.

All this discussion brings our notice to the fact that cyber security should be the prime concern at this hour when everybody is conducting their daily activities online. More usage of personal computers, desktops which are not so well equipped with security measures, not having firewalls installed at their ends, are making organizations data vulnerable to be theft or misused by attackers. Usage of Internet is not only benefiting us for seamless conduct of everyday act even staying indoors, but also imposing a greater risk of losing money, confidential information etc. if not taken proper security measures.

Measures to safeguard from Cybercrimes: Apart from making the networks and applications secure from the companies end, users can follow several mechanisms to safeguard their own virtual identity and ensure security. Privacy settings of the social media accounts should be kept in such a way that only trusted users can have access to the profile. Check unknown links in virustotal.com for any virus, malware or spam before accessing it. Check for misspelt website links to avoid siphoning attacks. It is always a good practice to access social media accounts from incognito browser windows. Users should report any telephone number or website link to the CERT-In (Indian Computer Emergency Response Team) if found suspicious, to stop further spread of any criminal intention.

Sources of Information:

https://www.aninews.in/news/national/general-news/aligarh-police-book-locals-councillor-for-beating-man20200417111213

https://timesofindia.indiatimes.com/city/hyderabad/cybercrime-cases-rise-in-hyd-amid-lockdown/articleshow/75149103.cms

https://timesofindia.indiatimes.com/business/india-business/cognizant-comes-under-maze-ransomware-attack/articleshow/75239553.cms

https://economictimes.indiatimes.com/markets/stocks/earnings/maze-ransomware-attack-to-hit-cognizant-revenue/articleshow/75251293.cms

https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/

https://en.wikipedia.org/wiki/Ransomware

https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams

https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams

https://www.bbc.com/news/business-52392084