# AN ANALYSIS OF THE COVID-19 IMPACT ON CYBERCRIME

Shobika. k, Sastra Deemed To Be University, Thanjavur, Tamilnadu

**ABSTRACT**

Individuals and society are very vulnerable as a result of the COVID-19 pandemic. We all rely more than ever during this crisis on computers, mobile devices, and the Internet to work, communicate, purchase, share, and receive information, as well as to help lessen the effects of social isolation. The majority of information is now available electronically and vulnerable to cyber threats in this age of digital processing. A wide variety of cyber threats exist, and their early activity might be difficult to interpret. These attacks might be carried out for a reason that has serious societal consequences, such as economic harm, psychological distress, a threat to national security, etc. Hackers now find cybercrime to be a lucrative method of causing havoc and disruption. To identify, investigate, attribute, and prosecute the aforementioned offences and bring individuals who take advantage of the COVID-19 pandemic for their own criminal ends to justice for that criminal justice authorities must work together.

## INTRODUCTION

Data flows via the internet have evolved into a pervasive phenomena in both the public and private sectors in this modern era of online processing, posing a serious issue at national and international levels. The term "cybercrime" was created as a result of human culture's deceitful attitude continuing to exploit the internet as a tool of violence. Due to the COVID-19 epidemic and the enacted lockdown, more individuals were confined to their homes, spending more time online daily and relying more and more on the Internet to acquire services that they would typically obtain offline.

## SHIFT IN FUNDAMENTAL FORM OF LIFE LEADS TO CYBER CRIME

The risks of cybercrime have existed for a long time, but as more people are using the Internet and spending more time online, along with the feeling of confinement, anxiety, and fear brought on by the lockdown, there are more opportunities for cybercriminals to exploit the situation and increase their profits or cause trouble. It is crucial to keep in mind that some demographic groups, such as youngsters, are more susceptible and require more online time for services like schooling. E-crimes have increased dramatically as a result of the fundamental shift in how we use the Internet and conduct our lives.

Common cybercrime methods like phishing have increased in frequency. Phishing is the dishonest technique of tricking people into divulging sensitive information, like passwords and credit card details, via fake websites or emails. New information obtained by Google and examined by virtual private network (VPN) service provider Atlas VPN is clarifying the extent of this. According to the research, Google identified 14900 active phishing websites in January. That amount nearly increased to 293k in February. However, that number rose to 522k in March, a 350% rise from January[1].

## INCREASE IN CYBER CRIMES

Cybercrime has risen during the epidemic, according to nations all across the world[2]. For instance, the Polizia Postale, the Italian law enforcement agency in charge of combating cybercrimes, recorded numerous scams and frauds that manifested themselves as

[1] https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine/
[2] https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

advertisements, emails, fake websites, as well as calls and text messages[3]. Cybercriminals are exploiting malware, such as viruses, worms, Trojan horses, ransomware, and spyware, to infiltrate, damage, steal, or erase personal data on personal computers by profiting on the concerns and fears brought on by the pandemic. Then, the stolen data can be utilised for a variety of malicious activities, such as accessing bank accounts and extorting ransom payments from the victims.[4] The Italian law enforcement agencies have also been alerted to a "Corona anti-virus" programme. The programme, called Black Net Rat, claims to shield the user's device from viruses, but instead compromises computer security and seizes control of the device, giving the criminal remote access to it[5].

On a growing number of websites well-designed by criminals, a rapid increase in fraudulent or inappropriate medications and medical equipment marketed at very high prices to purportedly cure the Coronavirus was observed. In relation to this, a rise in the trafficking of fake goods including hygiene products and face masks that are promoted via emails and websites was seen[6]. Additionally, the Italian Police claimed that in some instances, legitimate crowdsourcing projects to raise funds for healthcare facilities that have been under a lot of pressure over the previous few weeks were diverted to other criminal pockets using fake websites.

In these times of restriction, promises of bogus investment opportunities are still another typical fraud that occurs online[7]. This epidemic has spread throughout the world, and INTERPOL and the United Nations[8], have both issued warnings about specific online scams like this one connected to the COVID-19[9]. In the UK, there has also been an upsurge in frauds and attacks

[3] https://www.commissariatodips.it/da-sapere/per-i-cittadini-e-i-ragazzi/internet-rischi-e-minacce/index.html ( last visited Dec 10,2022)
[4] https://www.ilmessaggero.it/italia/coronavirus_reati_truffe_online_ultime_notizie-5111692.html https://www.ilmessaggero.it/italia/coronavirus_reati_truffe_online_ultime_notizie-5111692.html (last visited Dec 10,2022)
[5] https://www.techradar.com/news/corona-antivirus-infects-victims-with-malware and https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html?fbclid=IwAR13sai7vB5-_eBSRopHb0wqBqOX24i8hvhz3YOR06toRUMYVj6k3iV0Cpc and https://www.dqindia.com/cyber-crimes-surge-coronavirus-era/ ( last visited Dec 10,2022)
[6] https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation( last visited Dec 10,2022)
[7] https://www.scamwatch.gov.au/news/warning-on-covid-19-scams ( last visited Dec 10,2022)
[8] UN health agency warns against coronavirus COVID-19 criminal scams: https://www.uneca.org/stories/un-health-agency-warns-against-coronavirus-covid-19-criminal-scams ( last visited Dec 10,2022)
[9] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19 ( last visited Dec 11,2022)

aimed at businesses. For instance, emails purporting to be about the government's new award programme have actually downloaded ransomware or stolen money[10].

## IMPACT OF CYBERCRIME AMID COVID-19

A virus from the corona family known as Covid-19 was identified in 2019. Since December 2019, it has been spreading over the world as a result of close contact with an infected person. India has joined the majority of nations in declaring a pandemic, according to the World Health Organization[11]. The outbreak has become a major issue for businesses all across the world. Overnight, the demand for digital infrastructure has risen. This technology has given criminals a much bigger and more lucrative target. The global cyber threat environment has been significantly impacted by the extraordinary coronavirus epidemic.

One of INTERPOL's[12] private sector partners claims that between January and April 24, 2020, 907,000 spam emails, 737 malware incidents, and 48K dangerous URLs were discovered and were all linked to COVID-19. Additionally, from February to March 2020, there was a 220 percent increase in spam email and a 260 percent increase in dangerous URLs. Additionally, the top site for spotting spam and malware is in the United States. When the world locked down in March 2020, the overall number of Brute Force attacks against the Remote Desktop Protocol (RDP) jumped by 197%, from 93.1 million worldwide in February 2020 to March 2020, according to Kaspersky Telemetry[13].

## PREVENTIVE MEASURES TO HANDLE CYBERCRIMES

Our daily lives are reliant on technology in this digital age. Therefore, everyone in today's world is aware of and familiar with the Internet. The Internet offers all the information a guy needs in terms of data. People are consequently developing Internet addictions. Law enforcement agencies, the IT industry, information security organisations, Internet businesses, and financial institutions must build multifaceted public-private partnerships to effectively tackle cybercrime. In the virtual realm, cybercriminals do not contend for dominance or power.

[10] https://www.aljazeera.com/news/2020/04/uk-coronavirus-scams-online-doorstep-200414220652029.html (last visited Dec 10, 2022).
[11] Mayank Jindal and Dr. Vijay Laxmi Sharma, "Usability of Online Banking in India during Covid-19 Pandemic*", Int. J. Eng. Manag. Res.*, vol. 10, no. 6, pp. 69-72, Dec. 2020.
[12] *INTERPOL report shows alarming rate of cyberattacks during COVID19,* [online] Available: https://www.interpol.int/en/News-and-Events ( last visited Dec 11,2022)
[13] *Technology News: Latest Smartphones Mobile Phones Gadgets Tech Reviews Tech News,* [online] Available: https://www.businessstandard.com/technology (last visited Dec 11,2022)

Instead, they might collaborate to improve their abilities and even support one another occasionally. Therefore, we are unable to combat these cybercriminals using conventional anti-crime techniques. Despite cyber laws and government policies, there are a number of activities we should take to prevent cybercrime in our society.

## IMPLEMENT PREVENTIVE MEASURES AND RAISE AWARENESS

The expansion of COVID-19-related cyber threats is anticipated to continue posing legal and practical difficulties for law enforcement organisations around the world. Member nations are invited to develop comparable national awareness campaigns and to share the main messages of INTERPOL's worldwide #WashYourCyberHands campaign with their citizens on social media platforms.

**USING SECURE PASSWORDS**: Use unique password and username combinations for each account, and resist the urge to write them down. Cracking passwords using flaws is simple.

The following password combinations are more susceptible to hacking:

Passwords are generated using keyboard patterns. Think about xtedfhvdv.

Utilising easy combinations. jan2000, sara1999, etc.

Using the default passwords for the system. Hello123

**ENHANCE PUBLIC-PRIVATE PARTNERSHIP (PPP)**: Since the outbreak of the COVID-19 pandemic, PPP has been essential to successfully fighting the escalating cyber threats. By sharing knowledge and expertise on current trends and providing technological support, private sector businesses can be important allies for law enforcement agencies.

**PERMIT TIMELY INFORMATION DISSEMINATION:** The Cybercrime Directorate may effectively foresee forthcoming trends and broadcast the illegal tactics of an operation via the INTERPOL global network to increase awareness and combat cyber-crime when it has up-to-date information on recently identified cyber attacks. This is especially true when governments, critical infrastructure, and the healthcare industry are the targets of ransomware attacks, which can seriously jeopardise public safety and security. To safeguard the hardware and data:

Use the most recent version of antivirus software.

Techniques for cryptography (public key, private key) should be employed.

Users and emails that are mysterious should not receive a response[14].

**UPDATE YOUR SOFTWARE:**

With your operating systems and internet security software, this is extremely crucial.

In order to access your system, cybercriminals usually leverage known exploits, or flaws, in your software. By fixing those bugs and exploits, you can reduce your risk of being a victim of cybercrime.

**CONTROL YOUR SOCIAL MEDIA PREFERENCES:**

Secure your personal and private information. Cybercriminals who use social engineering can often obtain your personal information with just a few data points, so the less you share publicly, the better. For example, if you post your pet's name or reveal your mother's maiden name, you may expose the answers to two common security questions.

**IMPROVE YOUR HOME NETWORK:**

Starting with a strong encryption password and a virtual private network is a good idea. If cybercriminals do manage to breach your communication line, they will only intercept encrypted data. It's a good idea to use a VPN whenever you connect to a public Wi-Fi network, whether it's in a library, café, hotel, or airport.

**TAKE THE FOLLOWING PRECAUTIONS TO PROTECT YOURSELF FROM IDENTITY THEFT:**

Identity theft occurs when someone obtains your personal information unlawfully through deceit or fraud, generally with the purpose of gaining money. How? A thief, for example, may steal your mail in order to obtain access to account information, or you may be tricked into supplying personal information online. As a result, it is critical to safeguard your personal

[14] https://ieeexplore.ieee.org/document/9862935 (last visited Dec 12,2022)

information. A VPN, or virtual private network, can help to secure the information you send and receive online, especially when utilising a public Wi-Fi network.

**BE AWARE OF SIGNIFICANT SECURITY BREACHES:**

If you do business with a merchant or have an account on a website that has had a security breach, find out what data the cybercriminals acquired and modify your password instantly.

**DISCUSSION WITH YOUR KIDS ABOUT THE INTERNET:**

You don't need to restrict communication channels to educate your children what is and isn't relevant and beneficial behaviour. Make it clear to children that they may contact you if they face any online bullying, stalking, or harassment.

**WATCH OUT FOR THE CHILDREN:**

Along with discussing the internet with your children, you should also teach them how to avoid identity theft. Because children's Social Security numbers and credit histories typically symbolise a clean slate, identity thieves routinely target them. By being cautious while exposing your child's personal information, you can prevent identity theft. It's a good idea to be aware of the signs that could point to a breach in your child's identification.

**KNOW WHAT TO DO IF YOU BECOME A VICTIM:**

If you feel you have been the victim of a cybercrime, you must notify the local police and, in some situations, the FBI and the Federal Trade Commission. Even if the offence appears trivial, this is critical. Your report might help authorities with their investigations or prevent crooks from taking advantage of others in the future.

**CONCLUSION**

Additionally, this analysis outlines the most serious COVID-19-related cyber security concerns. We have also shed some light on the preventative steps that might be taken to stop cybercrimes. In order to lessen cybercrime, networking systems that protect people's sensitive personal data must be developed and put into place. Similar to this, awareness seminars should inform people about various types of cybercrime and how cyber security measures may be used to protect their data, especially women, children, and older people. Without a strong

commitment from all countries, it is almost impossible to eradicate cybercrime. To benefit from the digital world, we must protect ourselves against cybercrime and be cautious and aware of the most recent scamming techniques.