



COVID-19: A Pinnacle of Electronic Terrorism

Surbhi Bahl¹

¹Assistant Professor, Guru Nanak Dev University, Regional Campus, Gurdaspur (Punjab)

Abstract

In the time of Covid-19, there has been a tremendous loss of lives of people, but it has also impacted a large number of people. During this time, people have shown a lot of dependence on technology to carry out their tasks. There has been a vast area of e-transactions. The Internet is a tool that provides many services to people. Despite its various advantages, some people have tried to use it in a negative way. These days Internet is used as a tool for committing undesirable activities. Electronic terrorism is an illegal activity that is carried out through electronic mode. Anybody can be a victim of it. People can gain unauthorized access to your computer and steal your data by installing viruses. It can lead to service interference, eventually leading to financial losses. The hackers can misuse the information and make profitable gains from it. It is an upcoming issue. Weightage should be given to the installation of upgraded security and privacy measures. Cyber laws should be upgraded correspondingly to the current scenario.

Keywords: Electronic Terrorism, Privacy, Security, Virus, Transaction.

Introduction

There has been a vast adoption of electronic mode at the time of Covid. People were hands on their phones and used them to pass their time or carry out their work. There has been the adoption of electronic mode in the time of Covid-19. People are assessing it on a huge scale. It has engaged people during the period of lockdown. But they are also facing repercussions as hackers attack them. Cyber terrorism has hit people hard.

Examples of Cyberterrorism

1. E-stalking- It is a case in which the stalker monitors a person's online activities. The intention is to collect the information about the person and use it to harass them.
2. Inability to access service- In this case, people cannot access their account as someone has hacked it.
3. Theft of personal information- The personal information of a person can be stolen by a hacker and can be used for undesirable activities

4. Intrusion-The hacker gains unauthorized access to the computer system and creates disruption in services.
5. Email bombing-in this case large number of emails are sent to the recipient's email account in a very short period of time.The receiver will get irritated.

Ways to handle Cyber terrorism

- Limit handling- Donot unnecessarily scroll the websites as they can be ingenuine.Use the technology in a limited way.
- Strong Password-Change your password frequently. Your password should be a mix of alphabet, numerical and alphanumeric digits.
- Authentication- Install a multi-stage authentication system to keep a check on unauthorized login attempts.
- OTP- Never share your passwords or OTP with anyone.Avoid accepting any unnecessary requests.
- Applications- Donot download any apps from untrusted sources.

Major cases of electronicterrorismduring Covid-19

- Check Point Research, A Multinational cyber security company, has stated that up to12 May 2020, there were around 192, 000 cyberattacks every week related to coronavirus,
- In April and May, there were around 20, 000 new domains related to corona virus on the Internet, and 17% of these were malicious or suspicious.
- The data given by National Commission for Women (NCW) stated that in the month of March 2020, around 37 complaints were received online and by post.In the month of April 2020, the number of online cybercrimecomplaints rose to 54.
- The founder of the Akancha Foundation stated that they received 412 genuine complaints of cyber abuse from March 25 till April 25. Out of these, as many as 396 complaints were serious from women ranging from abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail, etc.

Impact of Electronic Terrorism

1 Impact on People

Electronic terrorism has increased the susceptibilityof people toward electronic threats. There is a shift of people to electronic due to the coronavirus. People have started using technology more responsibly as they are becoming aware of the repercussions they might have to face.

2 Impact on business houses

The business houses are already bearing many losses due to the pandemic, and electronic terrorism has made it worse for them.They have started monitoring the online platforms of their business to protect their goodwill.There is proper customer support to solve the grievances of the customers.

Conclusion

The Internet is the heart of many people, yet it has certain disadvantages. Cyberterrorism is very difficult to hold. It isn't easy to stop. Hence, the individual's responsible for making the best use of it. Preventive measures should be adopted individually to avoid any complexity. Websites should be accessed only from secured platforms. The user should avoid sharing their password with anyone to prevent theft and misuse of sensitive information. With the advent of the increase of online users, cyber terrorism might grow. The Government should make stringent laws for monitoring the activities and ensuring proper compliance.

References

- Stanicon, J. (2009), <http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html>
- Cybercrime. (2020, August 18). technopedia., <https://www.techopedia.com/definition/2387/cybercrime>
- Nwazor, T.(2016, October 13).5 ways tp Prevent Cyber Crimes From Dealing Your Business.Huffpost.<https://m.huffpost.com/us/entry/12450518>
- Steps for prevention of Cyber Crime.(2020, November26). Cyber Times. <http://cybertimes.in/?q=node/540>
- Laura.(2014, April 13).The Five Most Common Types of Cyber Crime.Supportz. <http://supportz.com/the-five-most-common-types-of-cyber-crime/>
- Define the five categories of cybercrime and give an example for each category. (2017, Novemeber 21). enotes. <https://www.enotes.com/homework-help/define-five-categories-cybercrime-give-an-example-478828>
- What is Cyber Crime.byenotes.com. <http://www.byte-notes.com/what-cyber-crime>
- Attack of the Hack Five of the worst cases of cyber crime of the world has ever seen from data theft of one Billion yahoo users to crippling the NHS. (2017, July 31).The Sun. <https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world- has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/>
- Be aware :20+ Email spoofing cases in India in 2016 may shock you.(2016, September12). Logix.<http://blog.logix.in/email-spoofing/>
- Sreedhar, N.(2020, June3).How Covid-19 became a fertile ground for cyber criminals. livemint.com. <https://www.livemint.com/mint-lounge/features/how-covid-19-became-a-fertile-ground-for-cyber-criminals-11591099416628.html>
- INTERPOL report shows alarming rate of cyberattacks during COVID-19.(2020, August4).interpol.int.<https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
- 'Significant' Increase In Cyber Crimes Against Women During Lockdown.(2020, May 3). NDTV.<https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352>

Kerala records highest number of cybercrimes during lockdown. (2020, May 21). The Economic Times. <https://economictimes.indiatimes.com/tech/internet/kerala-records-highest-number-of-cybercrimes-during-lockdown/articleshow/75865802.cms>

<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

<https://www.readynh.gov/disasters/cyber.htm>