International Journal of Applied Social Science
Volume 8 (10 - 12), October - December (2021) : 351-355
Received : 24.10.2021; Revised : 08.11.2021; Accepted : 24.11.2021

AN OVERVIEW
ISSN : 2394-1405 (Print)

DOI: 10.36537/IJASS/8.10-12/351-355

Rampant Cyber-attacks and Vital Security Measures: An Overview

ASHOK KUMAR
Associate Professor
Department of Commerce, Shyamlal College (Eve), University of Delhi, New Delhi (India)

ABSTRACT

Cybersecurity and the rising incidence of cyberattacks are becoming essential to modern life. The relevance of cybersecurity is growing as more and more people use the internet for various purposes, including business (Srinivas & Das, 2019). However, other cyberattacks, including one involving the ransomware virus, have been launched in recent years. As a result, the proper authorities must raise public awareness about the dangers of cyber assaults and the need for more robust cybersecurity. This brief article examines the rising tide of cyberattacks and the ways in which cyber defenses can protect individuals and organizations.

Key Words : Cybersecurity, Cyberattacks, Digital Protection, Global Connectivity, Security Threats

Today, one of the critical aspects of modern life is cybersecurity and the increasing number of cyber-attack cases. As more and more people are accessing the internet daily for several reasons, such as their work, the importance of cybersecurity cannot be undermined (Srinivas and Das, 2019). However, in recent years, various cyber-attacks have been carried out, and theransomware virus attack is one of them. Due to this, the relevant authorities must educate and spread awareness among people regarding cyber-attacks and the importance of cybersecurity. The short paper analyses recent cyber-attack trends and how cybersecurity can help safeguard people and businesses against such attacks and threats.

In recent years, the number of cyber-attacks has increased by a significant margin. It has become essential for the authorities to ensure that such attacks and issues are minimized to the greatest extent (Lallie, 2020). Managing and reducing cyber-attacks has become one of the critical priorities for the authorities as they focus on developing different systems and approaches that can help reduce these instances. Cyber-attacks have increased recently and emerged as the greatest threat to the public, businesses, and entities.

Cybersecurity measures have become indispensable in the wake of such an increase in cyber-attacks and their threats. Cybersecurity is an intriguing issue for associations and organizations of all sizes in each industry (Low, 2017). Every organization has various needs and experiences, so with the arrangements of digital protection patterns for 2019 and 2020, one can perceive a more significant number of changes in how the internet is used. Notwithstanding, a considerable amount of the rundowns do, at any rate, share some essential qualities. Moreover, as digital assaults keep expanding yearly, they all underscore the significance and requirement for better network safety guards. Phishing has been a staple of digital protection patterns records for some time, and it seems, by only some accounts, to be going anyplace at any point shortly.

However, phishing these days is not just about messages alone, and Email is, as yet, an unfathomably mainstream assault vector (El Mrabet, 2018). Cybercriminals are additionally utilizing an assortment of assault vectors to reach and stunt their planned casualties into playing out an activity — for example, surrendering individual data, login qualifications, or in any event, sending cash. Progressively, phishing these days includes general

How to cite this Article: Kumar, Ashok (2021). Rampant Cyber-attacks and Vital Security Measures: An Overview. *Internat. J. Appl. Soc. Sci.,* **8** (10-12) : 351-355.

SMS messaging assaults ("smishing"), everything from correspondences via web-based media stages, like LinkedIn, to phishing destinations to try and make calls with a live individual ("vishing").

Cell phones are also subject to security threats. Almost everybody, these days, has a cell phone in their pocket; and it truly is one of the most excellent portable devices to use the network, leading to it being subject to cyberattacks. Therefore, there is a need for a cellphone cyber security system. (Kimani and Oduol, 2019). Being portable, it makes life more advantageous. However, comfort does not come without hazards for end clients and organizations— mainly as more individuals utilize their portable gadgets, especially cell phones and work gadgets, reciprocally for individual and the organization's purposes. This trend explains worries for organizations.

In 2019, cybersecurity was a significant issue for the technology industry and the general public. It was one of the critical points on which governments and authorities in different countries were working. Attacks such as ransomware, credit card frauds, etc., were key cyber-security issues that affected governments, the public, and different businesses (Kavallieratos and Katsikas, 2018). In the wake of the fact that the world is fast moving towards an online integrated world, which means that pretty much all activities are being carried out using the internet and internet-enabled tools. The Internet of Things also emerged as one of the many ways different online activities were performed, yet ransomwareis a significant threat to online work.

Double Extortion was one of the key trends regarding cyber-attacks. It is a type of ransomware with a new strategy that makes the victims' files inaccessible. In recent years, the number of ransomware attacks has increased by a significant margin (Kavallieratos and Katsikas, 2018). This caused several issues for the general public and made them suffer from various issues and problems. The cyber attackers tended to make various files and folders of the victim inaccessible to them, and to access them; they had to make payment of a certain amount. When the victims refused to make such payments, the attackers could block their files permanently and even delete them (Srinivas and Das, 2019). Such attacks have increased significantly recently and have become a common trend.

The number, intensity, and scale of cyber-attacks have increased substantially. The intensity and scale of these attacks also have increased. There was a time when cyber warfare was carried out at a tiny scale, but their intensity and scale have emerged as a leading trend of increasing cyber-attacks (Lallie, 2020). These attacks are even more dangerous because artificial intelligence has evolved significantly. The traditional tactics to deal with such issues and the methods to gather intelligence and the required knowledge have also changed considerably as more people use hand-held devices and access the internet.

Attacks on mobile devices have also increased by a significant margin. Cybercriminals and attackers now target mobiles, as smartphones have become very common (Low, 2017). Almost every person uses smartphones daily; due to this reason, these devices contain much valuable information about the users, which hackers can use to their advantage and create issues for the users. Mobile devices are highly vulnerable to cyber-attacks, which are also a soft spot for cyber attackers. It has been observed that these devices can be attacked and hacked very quickly. Therefore, it can be said that mobiles are one of the preferred devices that cyber attackers tend to attack and use to destroy the lives of the users or the victims.

As the world is moving towards a web-based or online framework, the mists have risen as the main stages that can help individuals in playing out a vast assortment of undertakings effectively, alongside putting away a great deal of essential data that can be effortlessly gotten to at whenever from anyplace (El Mrabet, 2018). Enterprises needed to make fast foundation changes to secure their creation when working distantly. Much of the time, this was only conceivable with cloud advances. In any case, it likewise uncovered more misconfigured or essentially unprotected resources for the web. Moreover, just because, disturbing weaknesses were uncovered in the Microsoft Azure framework that could empower trespassers to escape the VM foundation and bargain with different clients. Thus, There have been numerous instances when one needs to be extra cautious about cyber-attacks.

In recent years, as cyber-attacks have increased at a very relatively rapid pace, the importance of cybersecurity cannot be understated. Today, it has become imperative for the authorities and experts working in this field to determine ways through which the security of the users can be increased. In this day and age, where almost everything is connected through the internet, the role of cybersecurity is crucial. Almost all information, such as banking, personal life, and many other forms, is stored on mobiles (Kimani and Oduol, 2019). Due to this reason, anyone who gains access to the mobiles of such individuals can gain access to their lives and even control them, leading to a greater need for cyber-security.

As the risk of cyber-attacks increases, the need and necessity of cybersecurity is increasing rapidly. Global connectivity and the use of cloud services are increasing rapidly, socybersecurity has gained significant importance in recent years (El Mrabet, 2018). Cyber threats can emerge out of any degree of association. Management should instruct the staff about basic social building tricks like phishing and more complex network protection assaults like ransomware assaults (like WannaCry) or other malware intended to take licensed innovation or individual information. Online protection is the state or cycle of securing and recouping PC frameworks, organizations, gadgets, and projects from a digital assault. Digital assaults are an inexorably complex and developing risk to touchy information. Assailants utilize new strategies fueled by social design and artificial consciousness to go around normal security controls. The world is progressively dependent on innovation. This dependence will proceed as one presents the up-and-coming age of brilliant Internet-empowered gadgets that approach our organizations through Bluetooth and Wi-Fi (Lallie, 2020). This has made network safety very important in today's world.

Network safety's significance is on the ascent. The general public is more innovatively dependent than ever in recent memory, and there is no sign that this pattern will slow. Individual information that could bring about data fraud is presently presented in general society on our online media accounts (Kavallieratos and Katsikas, 2018). Sensitive data like federal retirement aide numbers, charge card data, and financial balance subtleties are stored in distributed storage administrations like Dropbox or Google Drive. This has been a trend all across the world.

Whether an individual, an independent company, or an enormous worldwide, they consistently depend on PC frameworks. Pair this with the ascent in cloud administrations, helpless cloud administration security, cell phones and the Internet of Things (IoT), and various online protection dangers that did not exist a few decades prior. The world needs to comprehend the contrast between network safety and data security, even though the ranges of abilities are getting more comparative (Kimani and Oduol, 2019). The requirement is to safeguard people.

Today, cybersecurity is an essential part of modern-day life. It has become imperative for the experts and relevant authorities to develop and determine ways through which people's online security can be ensured (Kavallieratos and Katsikas, 2018). This entails developing various systems that can make this process much simpler and more effective. In this regard, the very concept of cybersecurity is fundamental. There are several ways through which cybersecurity can be maintained. One basic yet highly effective way is to encrypt and back up the data. Herein, as the name suggests, the focus is on keeping a backup of whatever data is stored on the device and encrypting it so that no other person or entity can access it. This is one of the critical elements to protect oneself from cyber-attacks.

Two critical elements in protecting against cyber crimes are preventing physical access and encrypting the data. Access to delicate and sensitive information can only be helpful if it falls into the righthands (Low, 2017). Organizations can accomplish the last by continually encoding their information. Information encryption remains the 'most proficient fix' for information breaks, should they happen. Make sure to scramble all touchy information, including client, worker, and business information. Full-plate encryption programming is remembered for all working frameworks today and can scramble all the information on a work area or PC. Additionally, watch that this product is enacted and refreshed on all organization gadgets. Furthermore, limit the time a PC sits unused and opened by setting all gadgets to enter 'rest' or 'lock' mode after five minutes of no utilization (Lallie, 2020).

Since cyber-criminals keep working enthusiastically to discover perpetually progressed methods of penetrating security safeguards, even the most security-cognizant organizations stay in danger of an assault. US investigation into the expense of information penetration has demonstrated that in 2017, the average worldwide expense of a solitary information break occasion was USD 3.6m – proportional to USD 141 for every information record (El Mrabet, 2018). The misfortunes brought about by information penetration are best moderated by putting resources into digital protection. However, 9% of UK and 15% of US organizations have this protection. The representatives must know the uses, even with protective measures against cyber threats.

Representatives are the most well-known reason that information penetrates the system. They cannot perceive outside dangers when they happen or do not have a decent comprehension of the daily activities that leave an organization helpless against an online attack (Lallie, 2020). Prohibiting representatives from utilizing their gadgets for work may appear to be a conspicuous methodology, yet this procedure only works in the short haul. As staff individuals become worn out with the burden, they will probably profit from getting to work for individual gadgets, paying little mind to approaches restricting this. It is more effective to show staff how to utilizetheir own and work gadgets to limit the danger of being hacked (El Mrabet, 2018). The head of the rundown should teach them about the dangers of utilizing unstable organizations to get work data to be cyber-secure.

To effectively use cybersecurity and its various features and aspects, it is of utmost importance for the relevant authorities to develop the appropriate infrastructure and provide the necessary facilities and tools. Developing and maintaining such an infrastructure can not only be very costly, but it can be a time-consuming process as well. Due to this reason, attention should be given to developing better ways of creating and maintaining such an expansive infrastructure (Srinivas and Das, 2019).

Despite huge online protection presentations, most entrepreneurs accept that their organization is sheltered from programmers, infections, malware, or an information break. This distinction is, to a great extent, due to the conviction that independent companies are the focus of digital assaults. Indeed, information hoodlums are just searching for the most straightforward course of action. Outside sources like programmers are not the primary way the organization can be attacked (Low, 2017). Little organizations have a family-like environment and put excessive trust in their workers. This can prompt a lack of concern, which is what a displeased or, as of late, terminated worker needs to execute an assault on the business.

Each new application can make way for a digital assault if they do not usually fix and update all products on each gadget the workers utilize. Continuously one should check for refreshes when buying another PC or introducing another product framework. Know that product merchants are not needed to give security updates to unsupported items. For instance, Microsoft® will quit supporting Windows 7 in January 2020, so if they have not redesigned at this point, presently is an ideal opportunity to do as such (Lallie, 2020).

Some other measures one can take for cyber-security involve trying not to defer downloading working framework refreshes. These updates regularly incorporate new or upgraded security highlights. Firewalls can defeat malignant programmers and prevent workers from perusing unseemly sites. Introduce and update firewall frameworks on each worker's PC, cell phone, and organized gadget. Incorporate off-site workers, regardless of whether the firm uses a cloud specialist co-op (CSP) or a virtual private organization (VPN). The firm may likewise need to introduce an interruption discovery/avoidance framework (IDPS) to give a more prominent degree of assurance (El Mrabet, 2018).

Moreover, one should find means to keep one's inboxes of mail in order. One should use email and internet browser channels to dissuade programmers and keep spam from obstructing worker inboxes (Kavallieratos and Katsikas, 2018). Organizations can likewise download "boycott" administrations to impede clients from perusing hazardous sites that present malware chances. Alert the representatives against visiting locales often connected with network safety dangers, such as explicit sites or web-based media. This may appear an easy decision; however, it just takes one worker to visit an inappropriate site to download malware onto the organization's frameworks incidentally.

In general, one should utilize full-circle encryption to ensure the safety of PCs, tablets, and cell phones. Spare a duplicate of the encryption secret key or key in a protected area separate from the far-away reinforcements (Low, 2017). Email beneficiaries ordinarily need a similar encryption capacity to decode. Never send the secret word or key in a similar email as the encoded report. Offer it to them using the telephone or some other technique. Thus, general safety measures should also be undertaken by everyone to safeguard oneself from cyber-attacks.

As more and more people are accessing the internet daily for several reasons, such as their work, the importance of cybersecurity must be maintained. In recent years, the number of cyber-attacks has increased dramatically, leading to many individuals and organizations being victims of cyber-attacks and crimes. It is time that people and organizations are made aware of the cyber-security measures to safeguard themselves against these attacks and at least minimize the possibility of being threatened at every step of their lives. Attacks such as ransomware, credit card frauds, etc., were key cyber-security issues that affected governments, the public, and businesses. When the world is fast moving towards an online integrated world, cyber-safety measures must be integrated into the cybernetic world and people's mindsets and uses of internet facilities.

REFERENCES

El Mrabet, Z. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, 469-482. DOI: 10.1016/j.compeleceng.2018.01.015.

Kavallieratos, G.and Katsikas, S. (2018). Cyber-attacks against the autonomous ship. *Computer Securit*, 20-36. https://doi.org/10.1007/978-3-030-12786-2_2.

Kimani, K. and Oduol, V. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 36-49. DOI:10.1016/J.IJCIP.2019.01.001.

Lallie, H. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv:2006.11929**.**

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security 2017*, 18-20.

Srinivas, J. and Das, A. K. (2019). Government regulations in cyber security: Framework, standards, and recommendations. *Future Generation Computer Systems*, 178-188.https://doi.org/10.1016/j.future.2018.09.063.

****