Email Security: Threats and Prevention

Vineet Kumar Chauhan[1], Chandan Kumar[2], Awadhesh Kumar[1], Jitendra Nath Shrivastava[2] and Rafeeq Ahmed[1]
[1]CSE Department, Kamla Nehru Institute of Technology, Sultanpur, India
[2]CSE Department, Invertis University, Bareilly, India

Keywords: Cyber Crime, Email Spam, Phishing Attack

Abstract: Presently the entire world is facing the problem of security of the email inbox. Users are being the trapped by hackers and crackers by different unfair practices. Normal users of these emails are not well versed with the internet, and they disclose their information very easily. We have observed that these types of ignorance led to financial loss, black mailing etc. We have also observed that people are reluctant to complain to the concerned authority. Cybercrime is increasing rapidly, and innocent people are being victim. This paper analyses the threats and addresses the important prevention techniques.

1 INTRODUCTION

In the field of data innovation, network protection assumes an indispensable part. Getting the data has gotten probably the best test of today. At whatever point we consider network safety, the main thing that rings a bell is 'Cybercrimes,' which are developing colossally consistently. There are numerous measures being taken by different governments and organizations to forestall these cybercrimes. Network safety assumes a significant part in that it incorporates everything identified with securing our delicate information, by and by recognizable data, individual data, information, and government and industry data frameworks from endeavored burglary and harm. Spam implies unconstrained mass messages that are sent by methods for email, messaging, or other progressed gadgets. Backers overall use it because there are no working costs past that of man- aging their mailing records. It could similarly occur over web conversations in talk rooms, web diaries, and even more actually inside the voice, (for instance, Skype). Despite being a clear unsettling in- fluence, spam can similarly be used to amass fragile customer information and has also been used to spread contaminations and other malware. Possibly the most extensively saw kinds of spam are email spam; the term is applied in other media to practically identical abuses: Internet, Cellular Networks, and VoIP stages. The kinds of spam depicted in (Iqbal et al. (2016) Iqbal, Abid, Ahmad, and Khurshid) figure 1. Chan et al. (Chan et al. (2015) Chan, Yang, Yeung, and Ng) depicts a broader meaning of spam, that spam is an undesirable message shipped off a beneficiary who didn't demand it. Today email spam is the most broadly perceived type of spam. According to the report (Bhowmick and Hazarika (2018)) of the Message Anti-Abuse Working Group (MAAWG), between 88–91 percent of spam messages were sent from January 2012 to June 2014. The continued with presence of unwanted web traffic is a cautious sign to industry and researchers are seeing this issue really. There are numerous kinds of spam accessible shows in sort 1 out of these we zeroed in on Email Spam.

1.1 Email Structure

Email or electronic mail is a strategy for trading data, for example, text (Ahmed and Ahmad (2019)), sound, video, picture, and so forth) between two clients or numerous clients through electronic gadgets, for ex- ample, cell phones, PCs, and so on The main email was sent by Ray Tomlinson to himself as a test email message in 1971 and the message composed was "QWERTYUIOP". Email gives a productive, ease, and continuous methods for conveying data to individuals (Ahmad et al. (2019) Ahmad, Ahmad, Pal, and Malviya). Each email

Chauhan, V., Kumar, C., Kumar, A., Shrivastava, J. and Ahmed, R.
Email Security: Threats and Prevention.
DOI: 10.5220/0010567500003161
In *Proceedings of the 3rd International Conference on Advanced Computing and Software Engineering (ICACSE 2021)*, pages 238-242
ISBN: 978-989-758-544-9

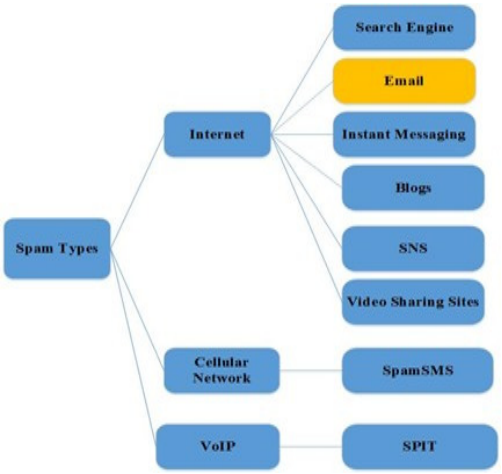

Figure 1: Types of spam

client is appointed its email account with an extraordinary name. This name is alluded to as the Email address. Various clients may send and get messages by email address. By and large, email is as username@domainname.
chandankumar@gmail.com, for instance, is an email ad- dress where chandankumar is the username and where gmail.com is an area name. Both the names are isolated by @ image. There are numerous areas are accessible, for example, yippee, hotmail, rediffmail and so forth and the whole space name follows their own terms and Conditions for the composing username segment.

1.2 Motivation, Contribution & Organization

In the current scenario, digitization is the aim of the nation. Digitization, when executed precisely, will show examples of advantages concerning cost and proficiency, for example, Increase in Productivity, Safe and Secure: Disaster Recovery, Environment Friendly etc. Incrementally, attackers also use different types of methods to harm the users. So, I focused of one of the common methods i.e., E-mail Security because with the help of email hackers one many type of scams. Hence this paper explored fundamental concepts of Threats and prevention form E-mail hacking. So user can aware and prevent them self from attackers.

2 RELATEDWORK

The email contains unstructured data where text mining is done (Ahmad et al. (2016) Ahmad, Ahmad, Masud, and Nilofer; Ahmed and Ahmad (2012)) and semantics are important (Ahmed et al. (2020) Ahmed, Singh, and Ahmad). In this literature review, we followed a process that focuses (Bhowmick and Hazarika (2018)) investigated content-based email spam sifting strategies. Utilized Machine Learning-based spam channels and their variations. Investigate the promising branches of most recent improvements by estimating the effect of Machine Learning-based channels.

(Karim et al. (2019) Karim, Azam, Shanmugam, Kannoorpatti, and Alazab) Study on Artificial Intelligence (AI) and Machine Learning (ML) techniques for canny spam email recognition. Investigated four pieces of E-mail structure (Shrivastava and Bindu (2014)) talked about hereditary calculation-based technique for spam email sifting. Closed GA can be a decent choice related to other email sifting procedures can give more powerful arrangement.

(Shrivastava and Bindu (2012)) Investigated Issues made by spam, Classifications separating procedures and measurable misfortunes happened because of spams.

3 EVALUATING VARIOUS THREAT TYPES

There are following kinds of email security penetrates of which organizations or exchanges ought to know:

3.1 Spam

“Spam” alludes to spontaneous business email (UCE) or spontaneous mass email (UBE) by means of web slang. Most regularly, spontaneous email incorporates promotions for administrations or products, however not many valid sponsors use UCE to publicize. The spam that is most regularly utilized incorporates (Shrivastava and Bindu (2014); Karim et al. (2019) Karim, Azam, Shanmugam, Kannoorpatti, and Alazab):

- Foreign bank tricks or extortion plans for advance installments.
- Phishing tricks
- Pyramid frameworks that incorporate MLM
- “Get Rich Quick” or” Bring in Money Fast” plans
- Advertisement for explicit sites.
- Software contributions for acquiring and sending UCE email addresses.

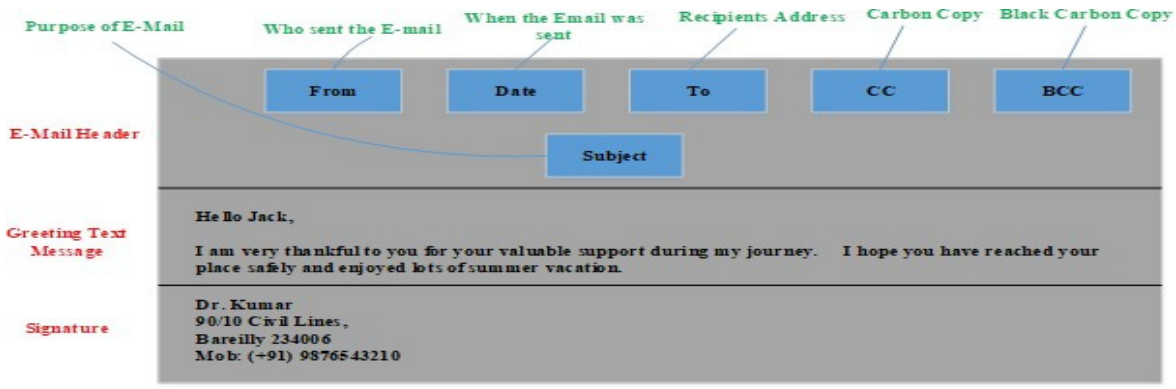

Figure 2: E-Mail Header

3.2 Phishing

It is a strategy where in programmers utilize electronic correspondence channels for the most part email to mimic a confided in figure. The beneficiary imagines that the message is coming from believed source and shared private data like the record subtitles or some time mentioned to open an unstable connection that causes hurt for them (Vaughan (2020)).

3.3 Malware

Malware, or malignant writing computer programs, is used by aggressors to pass on risks to affiliations that including contaminations, worms, Trojan horses, and spyware. Productive attacks give the malicious substance control over specialists and workstation, which would then have the option to be mishandled to change focal points or access delicate information or screen customers' activities and perform other poisonous endeavors (Shrivastava and Bindu (2012)).

3.4 Social Engineering

Aside from hacking a system, email is in like manner used to accumulate tricky information or get customers to perform exercises that further an attack. Email scorning, in which one individual or program adequately assumes the presence of another by tainting the sender data appeared in messages to cover the veritable root, is a standard social planning assault (Jensen (2020)).

3.5 Viruses

It is a PC program that adds noxious code to obliterate the getting gadget. Spam and phishing assaults are as often as possible followed by infections, utilizing email as a state of section from which they can get to the organizations of an individual or an association.

3.6 Insider Threats

A security hazard that begins inside the focused-on organization is an insider danger. This doesn't imply that in the organization, the entertainer should be a current representative or official. They might be a counsel, are signed specialist, a business partner, or an individual from the board (Rocha et al. (2020) Rocha, Souto, and El-Khatib).

3.7 Ransomware

It is another type of malware used to encode a casualty's records. It is a quite possibly the most pervasive types of digital assault there were more than 204mil- lion ransomware assaults in 2018. As per the network protection specialists at Norton, there are five kinds of ransomware (Anand and Sharma (2020)):

- Ransomware facilitated secretly for example Ransomware as an assistance.
- Responsible for the 2017 WannaCry ransomware assault for example Crypto malware
- Mimics the presence of antivirus programming, Scareware
- Threatens to distribute private or classified data in return for a payment for example Doxware.
- Lock you out of your PC for example Storage spaces

4 SPAMPREVENTION TECHNIQUES

The impact on an email security infringement can be destroying, from personal time and business interference to the deficiency of touchy data and reputational harm. Fortunately, to venture up their email security game, there are a couple of basic prescribed procedures associations can actualize:

- Invest in antivirus programming. The chance of email security infringement against our association can be essentially limited by an anti-virus program. It assists with securing our mail by fore- stalling the presence of noxious or undesirable messages by any means. It likewise shields our PC from infections that can erase our information, moderate our framework down or crash, or permit email to be sent by spammers by means of your record. Antivirus security checks for infections in our indexes and our approaching messages, and afterward disposes of something noxious.
- Implement a protected email passage. A safe email door or mail assurance passage" is intended to forestall the transmission of messages that break organization strategy, send malware or moved at a with noxious expectation." We can handle approaching and active email traffic and banner messages with sketchy connections by presenting a protected email entryway inside the as- sociation. At the point when joined with programmed email encryption, an ensured email door works best, which recognizes active messages containing possibly delicate or classified data and encodes them so programmers can't get to their substance on the off chance that they are blocked.
- Invest in a safe chronicling arrangement. As it is important for both administrative and legitimate purposes to set up a paper trail, most associations have some sort of framework set up that consequently saves email records inside a document. Yet, what occurs if it is anything but a steady chronicle? Everything necessary to get to a huge number of bytes of secret information and spot our business in danger is one programmer with the correct accreditations. Search for one that utilizes encryption, client validation, job-based authorizations, and more to make a multi-layered security technique when purchasing email chronicling arrangements.
- Create solid passwords and put resources into multifaceted validation. In spam counteraction techniques, strong passwords and multifaceted confirmation likewise assume an indispensable part. Email assurance possibly works on the off chance that it is paid attention to by every individual inside the organization and guarantees that specialists utilize solid passwords (for example a blend of various character types). Associations need to embrace a multifaceted verification system for added security, which permits clients to have at least two bits of proof to approve their character when entering their login qualifications.
- Be careful about each email connection. A straightforward route for programmers to spread malware and taint beneficiary framework is through email connections. Along these lines, de- spite the fact that it seems like it comes from a confided in source, it is basic that we cautiously investigate any connection prior to opening it. As a general guideline, records with two-fold augmentations or EXE expansions ought to be kept away from.

Apart from these techniques there are some basic ways to protect from spam

- Don't disclose email address publically
- Always think before click
- Don't reply any spam email
- Use spam filtering tool and antivirus software
- Don't use or share personal email address when registering for contest or other services.
- Detect and block the phishing websites

5 CONCLUSIONS

In this IT age, the communication mode is EMAIL. Everything sorts of all Communication must be assured. We have provided an understanding of the phishing problems and their implications to the com-mon people in order to resolve this issue. In or-der to identify, prevent and stop phishing, several re-searchers have offered different solutions. In this paper explored spam and their types and focused on E- mail spam. E-mail structure is also discussed.

REFERENCES

Alexy Bhowmick and Shyamanta M Hazarika. E-mail spam filtering: a review of techniques and trends. *Advances in Electronics, Communication and Computing*, pages 583–590,2018.

Asif Karim, Sami Azam, Bharani dharan Shanmugam, Krishnan Kannoor patti and Mamoun Alazab . A comprehensive survey for intelligent spam email detection. *IEEE Access*, 7:168261–168295,2019.

Jitendra Nath Shrivastava and Maringanti Hima Bindu. Trends, issues and challenges concerning spam mails. *International Journal of Information Technology and Computer Science (IJITCS)*, 4(8):10, 2012.

JitendraNath Shrivastava and Maringanti Hima Bindu. E-mail spam filtering using adaptive genetic algorithm. *International Journal of Intelligent Systems and Applications*, 6(2):54–60, 2014.

Muhammad Iqbal, Malik Muneeb Abid, Mushtaq Ahmad, and Faisal Khurshid. Study on the effectiveness of spam detection technologies. *International Journal of Information Technology and Computer Science (IJITCS)*, 8(1):11–21, 2016.

Patrick PK Chan, Cheng Yang, Daniel S Yeung, and Wing WY Ng. Spam filtering for short messages in adversarial environment. *Neurocomputing*, 155:167–176,2015.

Rafeeq Ahmad, Tanvir Ahmad, BL Pal, and Sunil Malviya. Approaches for semantic relatedness computation for big data. In *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*,2019.

Rafeeq Ahmed and Nesar Ahmad. Knowledge representation by concept mining & fuzzy relation from unstructured data. *published in International Journal of Re- search Review in engineering Science and Technology (ISSN 2278-6643) Volume-1 Issue-2*,2012.

Rafeeq Ahmed and Tanvir Ahmad. Fuzzy concept map generation from academic data sources. In *Applications of Artificial Intelligence Techniques in Engineering*, pages 415–424. Springer,2019.

Rafeeq Ahmed, Pradeep Kumar Singh, and Tanvir Ahmad. Novel semantic relatedness computation for multi-domain unstructured data. 2020.

Rikke Bjerg Jensen. Fragmented digital connectivity and security at sea. *Marine Policy*, page 104289, 2020.

Sakshi Anand and Avinash Sharma. Assessment of security threats on IoT based applications. *Materials Today: Proceedings*,2020.

Tanvir Ahmad, Rafeeq Ahmad, Sarah Masud, and Farheen Nilofer. Framework to extract context vectors from unstructured data using big data analytics. In *2016 Ninth International Conference on Contemporary Computing (IC3)*, pages 1–6. IEEE, 2016.

Thiago Rocha, Eduardo Souto, and Khalil El-Khatib. Functionality-based mobile application recommendation system with security and privacy awareness. *Computers & Security*, 97:101972, 2020.