Email Scam: The Worst Enemy for Human Beings

Abstract

Phishing is a cybercrime in which someone acting as a legitimate institution reaches a victim via email, telephone or text messages to attract their individuals to supply confidential data such as public identifiable information, financial and credit card numbers, and passwords. In this topic, I made a research about email scamming via online. Email scamming is one of the phishing methods and it has been existing since 1996. Phishing is a cyber-attack that uses disguised email as a weapon. Scammers made the same phishing links which are almost identical like they're from a company that people know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store that people are already keep in touch.. People easily trust those fake emails and they carelessly filled out all their personal information and bank account information. In this topic, there are some evidences and explanation about email scamming and how to avoid email spamming.

Introduction

Email is a short form of “Electronic mail” and was intended to share messages stored within a computer as a software. As far as programming is concerned, these are normally encoded using ASCII text. Email has been existing more than 50 years and still one of the first features ever available on the internet and still one of the most commonly used tools for different sites. Emails are a part of TCP/IP and which is a widely known protocol that has been using for sending and receiving messages. Email got a lot of advantages and disadvantages.

Advantages of email are Free delivery- sending emails does not cost any fees and no one has to buy email to use it is free of charge and it is free to use, Global delivery- Email can be accessed anywhere around the world and every users can be access from everywhere, Instant delivery- Emails are sent real time and are received by the recipient in almost instant, File attachment- Emails are not only free to use but also they can be sent with files such as images, documents, videos and mp3 files, Long-term storage – Emails can be kept forever and data is stored digitally, Resource-friendly- By using emails, people do not need to use physical resources such as papers and packing tape, which means that

there is no waste of resources. Therefore, these resources can be allocated to more pressing matters.

Disadvantages of email are impersonal- emails are via online so there will be lacks of talking over phone or meeting face to face, Misunderstandings- Email is just sending text and there is no tone of voice or body languages or facial expressions, Malicious Use- Emails can be sent anonymously which means can do cyber bully or upset people, Spam, Viruses – Email is one of the commonest ways for viruses to travel to every devices and those infected emails can be came from an anonymous source or sender or unknown contact, Pressure to Respond- people get annoyed if someone don't answer their email, Email Scam – Using fake email scam links or fake websites and hackers use fake websites constructed to look identical to real sites and try to trick to humans.

Nowadays, Phishing links are improving a lot and a lot of hackers and scammers use those links to steal users' information to hack. Phishing is a form of social engineering attack often used to steal user data, including passwords for authentication and numbers for credit cards. It happens when a person is duped into opening an email instant message, or text message by an attacker masquerading as a trusted entity. According to SocketLabs, history of email spam was sent by a man called Gray Thuerk on 3rd May 1978. He was working for Digital Computer Corp at that time and he sent an email request for an open house to demonstrate the company's new VAX computer. It went out about to 400 of the 2600 people and Thuerk claimed about $12 million.

Phishers start adopting HTTPS in 2017. If a user clicks on that phishing link, the site leads to – that try to trick user into entering credentials, personal information and phishers take all that information from user. In this modern technology, email scams become better and even professionals won't even notice that is fake or real message. According to this COVID-19 pandemic, phishers start to scam with popular themes such as Netflix scams or Spotify bill scams. Every country in the world has been affected by these types of attacks. In following paragraphs, there are more evidences and more way to prevent email phishing scams.

Cases:

Article 1

W. Z. Khan, M. K. Khan, F. T. Bin Muhaya, M. Y. Aalsalem and H. Chao, (2015), "A Comprehensive Study of Email Spam Botnet Detection," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2271-2295, Fourthquarter 2015, doi: 10.1109/COMST.2015.2459015.

Topic

W. Z. Khan, M. K. Khan, F. T. Bin Muhaya, M. Y. Aalsalem and H. Chao, (2015) discuss about that how the email communication system has been important and essentials for millions of people for several years. They also explain that spamming is information which is conveyed or distributed into a large number of recipients without informing them and spamming can be divided into a wide variety of classes like web spam, voice over internet protocol (VOIP) spam, mobile phone spam, messaging spam, email spam …. Etc.

Problems

The problem of email spam has grown significantly over the past few years and email spamming is not just a nuisance for users but also it is damaging for those who fall for scams and other attacks.

Method

They present detailed chronicles of spamming botnets which systematically describes the timeline of events and notable occurrences in the advancement of these spamming botnets.

Result

They aim to represent a comprehensive analysis of particular email spamming botnet detection techniques proposed in the literature. Also, they present a qualitative analysis of these techniques. By doing these process, they can do some challenges and future trends in detecting email spam botnets.

Article 2

Satheesh Kumar, M, Srinivasagan, KG, Ben-Othman, J. Sniff-phish, (2019): A novel framework for resource intensive computation in cloud to detect email scam. *Trans Emerging Tel Tech*, 2019 doi: https://doi-org.elibrary.jcu.edu.au/10.1002/ett.3590

Topic

Satheesh Kumar, M, Srinivasagan, KG, Ben-Othman, J. Sniff-phish, (2019) discuss about the cybersecurity threats and those threats can induce harm and to make illegal activities in a device or a network. Also, they explain about the phishing method and phishing method is the most potential threat in this cyberspace and phishing sites are mostly much intended toward an individual or a company, those kinds of phishing attacks are referred as spear phishing attacks.

Problems

The problem is email scam or phishing is a technique that most of the hackers use as baits to infiltrate into a system. They also said most of the scammers use email or test messages to trick people into giving them their personal information by sending spam phishing email. Phishing emails look like they are from a company that people might know and trust. Sometimes they might look like from a bank or a credit card company or online payment company. Ben-Othman provide that the FBI's internet crime complaint canter reported that people lost $57 million to phishing schemes in one year.

Method

In this paper, authors made an analysis that most of the people use their email by using Google Chrome or Mozilla Firefox but most of the business workers use Google Chrome. By using internet web browsers, they found a Chrome Extension application named Sniff-Phish. By using that extension application, they hope that they can reduce email phishing scams.

Result

Authors believe that using Sniff-Phish Chrome Extension application, they could be able to detect various categories. Of real-time email scams or phishing attacks like zero-days and spear phishing. This extension application is based upon analysing some basic criterion of the malicious URL and duly presenting the legitimacy level of the link in the form of a report.

Article 3

Almaatouq, A., Shmueli, E., Nouh, M., Alabdulkareem, A., Singh, V. K., Alsaleh, M., Pentland, A. (2016). If it looks like a spammer and behaves

like a spammer, it must be a spammer: Analysis and detection of microblogging spam accounts. *International Journal of Information Security,* 15(5), 475-49. Doi 10.1007/s10207-016-0321-5

Topic

Almaatouq, A., Shmueli, E., Nouh, M., Alabdulkareem, A., Singh, V. K., Alsaleh, M., Pentland, A. (2016) provide that Spam in online social networks (OSNs) is a systemic problem that imposes a threat to these services in terms of undermining their value to advertisers and potential investors, as well as negatively affecting users' engagement . They also said that as social media continues to grow according to popularity, spammers are increasingly abusing media purposes.

Problems

Authors said that as social media is improving a lot there will be more bot spams. They found an evidence that on Twitter, there are over 100 millions spam messages were collected within one month. But they found some ways to fix and they provide that two behaviourally distinct categories of spammers and that they employ different spamming strategies.

Method

On the other side, they analysed the detectability of spam accounts with respect to three categories of features, namely content attributes, social interactions, and profile properties. They suggested to use two some tools to prevent that spam messages. Those tools are SocialOoph and Socialtoo.

Result

By using those tools, they can prevent spam message bots and plan to further investigate the differences between the spam accounts utilizing other inter- actions functions (e.g., hashtag, retweet, and favourite). They also intend to quantify the success of spam campaigns and explore the tools, techniques, and spam underground markets utilized by spam accounts to spread their content and evade many of the known detection mechanisms.

Article 4

Sheikhalishahi, M., Saracino, A., Martinelli, F., La Marra, A., Mejri, M., & Tawbi, N. (2019). Digital waste disposal: An automated framework for analysis of spam emails. *International Journal of Information Security,* 1-24. doi:http://dx.doi.org.elibrary.jcu.edu.au/10.1007/s10207-019-00470-x

Topic

Sheikhalishahi, M., Saracino, A., Martinelli, F., La Marra, A., Mejri, M., & Tawbi, N. (2019) said that email spamming is one of the best-known and most annoying issues present on the internet in these days. They explained about the grouping and they purpose an automated methodology and the resulting framework based on innovative categorical divisive clustering, used both for grouping and for classification of spam messages.

Problems

They point out that spam emails cause several problems and spam emails are an effective tool to perpetrate different cybercrimes, such as phishing, malware distribution, or social engineering-based frauds.

Method

To this end, in this work they have purpose the CCTree algorithm for both clustering and classification of spam emails. The purposed algorithm has been developed in two versions so that they can detected how spam emails come to people.

Result

As the purpose of the algorithm is developing more and more, they can make an additional step toward the solution of the issue of spam, not only to emails, but also to other channels such as telephony, and online social networks which are today becoming a main channel for spam messages.

Article 5

Williams, Emma J., Beardmore, Amy., Joinson Adam.,(2017). Individual differences in susceptibility to online influence: A theoretical review : *Computers In Human*, 412-421,
Doi: https://doi.org/10.1016/j.chb.2017.03.002

Topic

Williams, Emma J., Beardmore, Amy., Joinson Adam.,(2017) provides that as mobile technology and computer communication has been facilitating rapidly and as those things become better, online scammers are growing. They pointed out that scammers successfully persuade people to click with malicious links, make fraudulent payments, phishing links and by downloading fake bank receipts. In this article, they presents a. theoretical review of literature relating to individual difference in online contexts.

Problems

Authors pointed out that social media platforms are also allowing online scammers to identify information and allowing scams to become increasingly personalized and effective. Also, people do not have enough about phishing and they also easily trust about those phishing links and email scam links.

Method

Authors shows some protection steps for people. Firstly, people have to protect your computer by using security software. Secondly, protect their mobile phone or computers by setting software to update automatically. Thirdly, they have to protect their accounts by using multi-factor authentication and finally, they have to keep data backup with external disks or on cloud storage.

Result

Authors have also highlighted a number of open questions regarding susceptibility to online influence that require further investigation and clarification.

Article 6

Idris, Ismaila (2015). "A combined negative selection algorithm–particle swarm optimization for an email spam detection system". *Engineering applications of artificial intelligence* (0952-1976), 39, p. 33.

Topic

Idris, Ismaila (2015) discuss that how Email is important for people. As the email is improving, photos and videos are attached together, and only real time protection mechanism can protect these spam pictures and videos. Author introduces an email detection system that is designed based on an improvement in the negative selection algorithm.

Problems

There are several major problems with email spamming. First problem is that spam email take a lot of space and fill in mailbox of users. Second problem is that there is no relationship between collectors' zone of interests and the substance of spam sends. Third problem is they cost cash for ISPs in light of the fact that the transfer speed and the memory of framework are squandered. Finally, Spam messages cause a great deal of security issues in light of the fact that a large portion of them incorporate Trojan, Malwares, and infections

Method

The authors pointed out that they will use the NSA model and NSA-PSO model to fix this problem. Authors show some steps that can fix this spam bot problem. The NSA-PSO detector for spam material takes input messages and verifies them with the files present in the database. The verification is performs message after message by measuring the various probabilities of spam occurrences to decide the spam material.

Result

Authors discuss that these model offers client sensitivity and may very well respond to changes in spam strategies in the future by recognising the spam material in a network through spam message modifications.

Article 7

Zhou, B., Yao, Y. & Luo, J. (2014) Cost-sensitive three-way email spam filtering. *J Intell Inf Syst* **42,** 19–45 (2014). https://doi-org.elibrary.jcu.edu.au/10.1007/s10844-013-0254-7

Topic

Zhou, B., Yao, Y. & Luo, J. (2014) discuss about cost-sensitivity email spam filtering and they divided into three-way email spam filtering so that it would be easier to demonstrates a better performance. They also provide users with a more meaningful way of treating their incoming emails with care. They also concentrate on two topics that are less studied, namely the computation of thresholds needed to identify the three email categories and the understanding of the cost-sensitive features of spam filtering.

Problem

Generally, authors discuss about the ternary email spam filtering. The ternary email spam filtering typically applies a boundary region to the results of the classification. They found more analysis that all emails cannot be easily identified are transferred from the positive and negative regions. They claim that certain levels ought to be inferred from a theoretical and realistic basis.

Method

They divided into three email categories. Instead of providing thresholds based on an intuitive understanding of the degree of error tolerance, the thresholds are determined systemically on the basis of decision-theoretical rough model collection models. They believe that diving into three categories can reduce the thresholds of email spamming. All these methods are well established from Bayesian decision theory.

Result

Instead of providing the thresholds based on intuitive understanding of error tolerance levels, the thresholds are determined systematically on the basis of decision-theoretical rough model collection models.

Analysis:

Email scam attempts aren't a new threat. According to Ismaila (2015), These scams have been circulating since the mid- '90s. But in 2020, they have become more and more sophisticated, have target every standard of people and have caused more harm to both individuals and organizations.

According to some researches, email scams are also kind of phishing methods and there are some ways to prevent those scam attempts. Most of authors suggested to install third party anti-phishing apps or chrome extension antivirus software because most of the users use internet browsers to use their mailboxes. So that using third party prevention applications will also be helpful for users to prevent. Some researchers suggested to use email filtering because good email gateways are used to filter out harmful and malicious emails and redirect them dynamically away from user inboxes. 99.99 precent of spam emails will be blocked. By a successful email portal and any email that contains any malicious connections or attachments will be deleted. This ensures that they are critical in keeping consumers from receiving phishing emails that are fake. These ways can also prevent email scams.

In my opinion, to prevent email scams, user should always keep inform about phishing techniques because email scams are kind of phishing and users should keep their eyes for news about new phishing scams. By finding out about those scam attempts, users will be at much lower risk of getting snared by one. Secondly, users should have common sense and think carefully before those email attempts. One of the most important things is not to turn off the firewall of the user's computer because high quality firewalls act as buffers between user, his or her computer and outside intruders.

Conclusion:

Overall, Email Scamming is a significant threat to all users of the internet, and it is impossible to track or protect against, since it is not clearly malicious in nature. Everyone has to look out for it and it mostly happens to everyone and if a person got scammed, it will cost a lot. Be alert and always keeps your eyes and ears open to something that even sounds distant, for it could well be scammers searching for their next target.

References:

1. W. Z. Khan, M. K. Khan, F. T. Bin Muhaya, M. Y. Aalsalem and H. Chao, (2015), "A Comprehensive Study of Email Spam Botnet Detection," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2271-2295, Fourthquarter 2015, doi: 10.1109/COMST.2015.2459015.

2. Satheesh Kumar, M, Srinivasagan, KG, Ben-Othman, J. Sniff-phish, (2019): A novel framework for resource intensive computation in

cloud to detect email scam. *Trans Emerging Tel Tech*, 2019 doi: https://doi-org.elibrary.jcu.edu.au/10.1002/ett.3590

3. Almaatouq, A., Shmueli, E., Nouh, M., Alabdulkareem, A., Singh, V. K., Alsaleh, M., Pentland, A. (2016). If it looks like a spammer and behaves like a spammer, it must be a spammer: Analysis and detection of microblogging spam accounts. *International Journal of Information Security,* 15(5), 475-49. Doi 10.1007/s10207-016-0321-5

4. Sheikhalishahi, M., Saracino, A., Martinelli, F., La Marra, A., Mejri, M., & Tawbi, N. (2019). Digital waste disposal: An automated framework for analysis of spam emails. *International Journal of Information Security,* 1-24. doi:http://dx.doi.org.elibrary.jcu.edu.au/10.1007/s10207-019-00470-x

5. Williams, Emma J., Beardmore, Amy., Joinson Adam.,(2017). Individual differences in susceptibility to online influence: A theoretical review : *Computers In Human*, 412-421,Doi: https://doi.org/10.1016/j.chb.2017.03.002

6. Idris, Ismaila (2015). "A combined negative selection algorithm–particle swarm optimization for an email spam detection system". *Engineering applications of artificial intelligence* (0952-1976), 39, p. 33.

7. Zhou, B., Yao, Y. & Luo, J. (2014) Cost-sensitive three-way email spam filtering. *J Intell Inf Syst* **42,** 19–45 (2014). https://doi-org.elibrary.jcu.edu.au/10.1007/s10844-013-0254-7