Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 3; April-June, 2016, pp. 204-206
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Email Security Concerns: Review and Analysis

Jitendra Nath Shrivastava[1] and Jaya Kushwaha[2]

[1]Invertis University
[2]M.Tech Student, Invertis University
E-mail: [1]jns@invertis.org, [2]jayakushwaha93@gmail.com

Abstract—*Presently all the websites of different organisation forces their users to input e-mail addresses for the identification of their entity. Our study reveals that the serious issues related to use of e-mail addresses as an identity and the associated online behaviours of users have not been well examined in the available literature. This paper discusses and analyzes security and privacy problems and threats resulting from the use of e-mail address as identity. Results illustrate that using e-mail address as an identity poses high security and privacy risks. This is mainly because of the multiple usages of e-mail addresses and users improper online habits. Moreover, the solutions for such e-mail threats are discussed.*

Keyword*:-Spam, Antivirus, Intruders, Hackers, e-mail, security and privacy, Security Threats*

1. INTRODUCTION

Email security basically means the combination the steps or measures taken to secure the access and protect the content of an email account or service. It permits individual or organization to preserve the entire rights over the several emails addresses. One who provides the email services equipment it with the email security services to secure protect the individual's credentials data from hackers. Email security basically consists of various ways to secure an email service. From an end user point of view, a practical email security measures includes:

- Strong passwords
- Password rotations
- Spam filters
- Desktop-based anti-virus/anti-spam applications

Likewise, the one who provides all such services make sure about the email security by using password and access control on an email server, encryption and digital signature of email are done when the messages come in the inbox or are in transit state either from any person or to any person's email address. Software based spam filtering and firewalls are also used so that it could restrict unwanted, unreliable, malicious email messages from being delivered to the user's inbox.

Email is most important tool which is been used in today's economic world, but it could create number of security threats, in both the way either it is incoming messages or outgoing messages. The incoming messages could be spam message or spoofed message which could cause chaos to your data, as it may contain number of malware as in attachments or fake links. Same is with the messages that are been send, they are not protected properly then it may expose once important and sensitive data to the intruders.

In brief, all of the email gives number of threats. Due to which a complex level of email security is needed for organisation and business. On the server level it is required to enhance the enterprise-level security. Given below are the following tools which are used to ensure email security across servers:

- Encryption techniques: Businesses related to the legal and medical offices, needs an efficient and complex type of encryption for their email security. In other conditions, IT managers would need to empower their level of protection. To make the communication more secure and protected Encryption systems are installed on the server.
- Filtrations of spams: Spam is a wicked reality of email. Providentially, many spams are not harmful, and by installing a filtration software on the mail server would try to remove all of the spam messages. This will, consecutively, remove many possible links in the mail.
- Attachment scanner: Attachment scanners try to terminate the harmful code before it gets executed. On installing the attachment scanner in the email server every attachment is checked or scanned to find the possibility of threats. If any of the threats are found they are deleted.

On the basis of different software installed in the different platform number of tools can be available for such security. Third-party method can also be used according to the security needed.

If one has the business or office then they don't need to install such heavy weighted servers but they should take some other important steps to protect their systems and information by installing security software like antivirus antispyware on every system of the office that are used to access the information of the company. Many of the email service providers offer many kind of the spam filter for mail service. Open PGP can be equipped easily if we see from the applications point of view.

Everyone should also use their literacy and common sense if they really wants to make their email account even more protected, either they are looking for the small business or an organisation. The biggest mistakes that any person could do are to get manipulated to click on any malicious link or attachments. To cope up with this mistake the people should be educated about the real meaning of such links how they look like and what should be done to them.

Nowadays one cannot even trust the email with the known sender name. That's the biggest thing that people should know about. Because if once they will add such fake people in their contact list they will spoof all the information and other contacts, and it may happen that such virus could move other mails in the contact list.

Now the question arises that what one should do when they face such conditions? Number one, you should not click on the suspected emails or links. Secondly, report about it. In addition to this command, teach every person of the office to scan the attachments whenever they get any. One can also use the blocker for the websites and advertisements filters. Using the sites such as torrents and etc should be prohibited as they work as open invitation for the threats.

Whether you're protecting a single computer or a network of thousands, many of the same principles of email security apply. A combination of tools and common sense should provide efficient protection and coverage, but one should always keep this in their mind and remember — if it seems to be doubtful, don't click on it.

This paper presents a view of the current state of social academic and industry solutions that can protect email users from various security threats. More importantly, this study give the following contributions: First, we outline the email security threats that target every user of mailing services, with an additional focus on email security Second, we present a detailed overview of the existing solutions to these threats, specifically those provided by email service provider, commercial companies, and academic researchers. Third, we compare and discuss various ways to protect the email and there solutions . Lastly, we give easy-to-implement recommendations on how email users can protect email.

2. TYPES OF THREAT

Malware: the malware are those type of the software which are made to damage the computer system so that it can get the user's personal details like its credential and access to its information. The malware uses the email to propagate among the different user by which it could attack other computers.

Phishing: the phishing attacks are example of the social engineering to get the information about the users by impersonating as a trust worthy third party. Usually people trust such emailing sites a lot and give away all their information to the email service provider and therefore, easily get attacked.

Spammers: spammers are the individual who uses the email services to send the fake messages or fake advertisements to any user of the email. The spammer could use comment messages to abuse or to hurt some once image publically.

Cross Site Scripting: the cross site scripting attack is a kind of assault on the web base application. The attacker who does such of the attack wants to exploit the trust of the web user by the web application as it makes the user to unknowingly download the infected code from the web and run it on its system through which the intruder could become able to get the information of the user.

Clickjacking: it is an attack which makes the user to click something different which they actually intended to click. By this technique the user unknowingly start posting spam message on their email

Identity clone attacks: By this attack the attacker tries to clone the presence or we may say the identity of any other person on whom the attacker wants to attack

3. SOLUTIONS

In this section the paper suggests some sort of the solutions which focuses on the identification of the malevolent user and the applications that could harm the user in several ways. These solutions are helpful in improving the privacy setting.

Improvement of the privacy setting interface: By the modification of the interface of the privacy setting the user becomes able to improve their privacy security on their self. The user could decide who could access their email and to whom the their information would be visible.

Phishing detection: Many methods have been suggested for identifying and preventing the phishing attacks. Basically these methods try to identify the phishing websites and phishing URL. For example a method was introduced in which the phishing attack was handled by redirecting to the different URL.

Spammer detection: several methods of spam detection have been proposed like the detection of video spammer, detection of spams using contents and network graph properties. Number of machine learning algorithms was also suggested for detection.

Cloned profile detection: The cloned profile could be detected by checking the occurrence of the duplicated or fake credentials. A method was introduced in which the software investigate whether the user's id is cloned or not by the help of the login ip record.

Avoiding the information /location leakage: Many methods were proposed to avoid the leakage of the information about the users by adding the access control mechanisms. But the most important thing that a user should understand is that they should take care about till what extend they should share their information

4. CONCLUSION

Emails have become a part of our daily life, as one could communicate, share and exchange their important information by the mean of email. On the other hand the emailing services could be dangerous also as the users consider it as most trust worthy service and voluntarily gives away all their information. The hacker, fraudsters, and online predators retrieve the user's information, so that they could misuse it for their goals. This paper tries to explain some types of threats that could occur through the email.

The paper also suggests some of the solution to protect against these online threats. It is not necessary that these solutions could provide complete protection to the users. Therefore it is important for the users to stay attentive before taking any action on the email either clicking on a link or downloading any attachment. The user should also be very sensitive about what kind of the information they reveal on the email so that no one could be able to get their important information so easily

As the concern for the future work in the direction of this research the email security is vast area on which one could explore, by finding more new generation threats and then developing so solutions to them. The email services are extremely important for everyone as it is considered as the once identity therefore, we should take accurate precautions to conserve our security.

5. ACKNOWLEDGEMENTS

I would like to thanks Prof. Jitendra Nath Shrivastava for proofreading this article and editing expertise and endless helpful advice which guided this article to completion.

REFERENCES

[1] Online Social Networks: Threats and Solutions Michael Fire, *Member*, *IEEE*, Roy Goldschmidt, and Yuval Elovici, *Member*, *IEEE*.

[2] Effectiveness And Limitations Of E-Mail security Protocols M. Tariq Banday P. G. Department of Electronics and Instrumentation Technology University of Kashmir, Srinagar - 6, India

[3] Security and Privacy Risks of Using E-mail Address as an Identity Lei Jin, Hassan Takabi, James B.D. Joshi School of Information Sciences University of Pittsburgh Pittsburgh, PA, US lej17@pitt.edu, {hatakabi, jjoshi}@sis.pitt.edu

[4] M. Fire, D. Kagan, A. Elyashar, and Y. Elovici, "Friend or foe Fake profile identification in online social networks," arXiv preprint arXiv:1303.3751, 2013.

[5] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots+ machine learning," in Proc. 33rd Int. ACM SIGIR Conf. Res. Dev. Inf. Retrieval, 2010, pp. 435–442.