Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 10, October-2021

A Review of Social Engineering Attacks and their Mitigation Solutions

Ansh Mehta
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India

Dev Vora
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India

Harsh Sachala
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India

Jay Khatri
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India

Dharmil Gada
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India

***Abstract*— The rapid growth in the internet has encouraged mankind to extensively use mobile phones, computers, and laptops for our convenience. From our day-to-day schedule to our conversations and financial information, all resides into our electronic devices and hence securing them would be of utmost importance for us. With all the data in our electronic devices and internet being so vulnerable, the cyber attackers are always trying to get access to our private and important data.**
This paper aims to bring into light the different methods and techniques employed by the cyber attackers and criminals to commit cybercrimes and harass the victims. It discusses the various kinds of attacks that can lead an individual to fall prey to the attackers, why humans are a weak link in cyber-attacks, the various counter-measures available and the role of AI, ML and in preventing these attacks.

Keywords*— *Social Engineering; Attackers; Phishing; Data; Cyber Attacks; Cybercrime.

1. INTRODUCTION

There's a standard pattern that may be related to social engineering attacks. As per Malcolm Allen (2006), this pattern may be stated as 'The Cycle'. The first step is to accumulate data regarding the victim; the second is to observe and build the connection with the target; and therefore the third step is to use the data gathered within the previous 2 stages. It then takes to hold out the attack. The offender disappears while not a trace at the fourth and end. The four steps of a social engineering attack square measure portrayed within the below Figure 1.

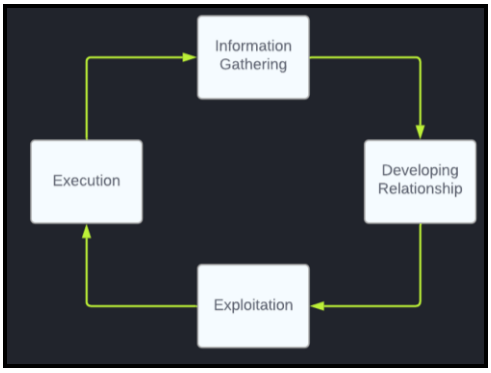

Figure 1: The Cycle

1.1 Social Engineering

The attacker's capability to hunt and gather the data that the victim desires by utilising the victim, exploiting human flaws is that the basis of the attack, and therefore the offender obtains personal and sensitive data regarding the individual or organisation is defined in concert of the straightforward techniques. By luring them to transfer malicious files and computer code, by clicking on malicious links, or downloading harmful applications that serve the offender to reveal the information, social engineering may be a technique that aims to control and track victims into accessing personal data, revealing their information, and trying to hurt a personal or organisation by luring them to transfer malicious files and computer code, by clicking on malicious links, or downloading harmful applications that serve the offender to reveal the information.

1.2 Social Engineering Attacks

One of the foremost serious and vital dangers and issues in cyber security is social engineering assaults. It will collect personal and sensitive data through social engineering, which may then be utilized for explicit reasons like blackmailing the victim or marketing it on the black market. In terms of aim, target, and principle, social engineering assaults dissent from each other, however all of them follow the same pattern of 4 set or allowable phases for attackers.

2. TYPES OF ATTACKS

2.1 Phishing Attack

This is the most basic type of social Engineering attack.Phishing attacks are the victim's attempt to fall into a fishing net in order to obtain confidential information and reveal sensitive data, and the victim is phishing through several methods of sending e-mail or phone calls, and includes malicious sites, fake prize announcements, fake offers, fake online shopping sites, and a variety of other methods and tricks used by the attacker to track down the victim. For example, you received an award with us to obtain the reward, click on the link and fill your data and bank card numbers, as well as secret numbers, or input any sensitive

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 10, October-2021

and private information that benefits the attackers and serves them online.

A. Spear Phishing:
Phishing attacks target an individual or organization, which is why spear phishing attacks are phishing fraud that defrauds an organization, group, or individual, by targeting an individual or group concerned with his name, and then collecting and searching for all that reveals to them the individual or group through the data available online. This kind is more difficult to differentiate from any legitimate user than the other sorts in phishing campaigns.

B. Whale Phishing:
The second kind, whaling phishing, is a subset of spearfishing that targets high-ranking executives in corporations and organizations, such as the CEO or CFO, in order to acquire sensitive and critical information.

C. Vishing and Interactive Voice Response Phishing:
The third and fourth types of phishing attacks are called Vishing, and they are based on speech fraud. This assault is defined as a deceptive statement that asks the victim to reveal sensitive and personal information via interactive answers, to which the victim responds phonetically. Following the victim's reaction over the Internet protocol, these assaults were carried out (VoIP).

D. Business Email Compromise:

The fifth form of phishing is known as business email compromise phishing (BEC). It's an assault that goes through whale phishing, which was mentioned in the third kind since it targets large characters. This kind works to get the authorization to enter email, gain access to calendars, and private information such as payments and accounting, as well as personal and sensitive information from those individuals.

2.2 SMiShing Attack

SMiShing is a sort of phishing assault that uses fake SMS messages to deceive unsuspecting victims into handing over sensitive information. This type of phishing is less frequent in the corporate sector than spear phishing and Vishing, but it is becoming more of a concern as the usage of bring-your-own-device (BYOD) in the workplace grows.
The majority of SMiShing attempts follow one of two patterns: The attacker encourages their victim to visit a URL given to them through text message. The URL then redirects users to a phoney credential logging page or a download page that downloads malware onto the user's computer.
Regarding the substance of the communication, the attacker invites their victim to contact a certain number. These calls may end in the attacker asking for sensitive information over the phone, as in a Vishing attempt, or they are made to a premium rate phone line, resulting in a high phone bill for the user.
When it comes to SMiShing, attackers frequently mimic brands in order to earn their victims' confidence. According to Check Point, Microsoft is the most imitated brand in the world, with 43% of brand phishing attempts utilising the Microsoft name, followed by DHL (18%), LinkedIn (6%), and Amazon (3% to 5 %). With more people than ever relying on Microsoft's cloud apps to build a virtual office, it's simple to see why attackers are taking advantage of their brand.

2.3 Pretexting
Pretexting is a way of fabricating a situation in order to persuade victims to reveal information they should not. Pretexting is frequently used against businesses that keep client information, such as banks, credit card firms, utility providers, and the transportation sector. Pretexter impersonate clients to get information from businesses, generally over the phone. Pretexting takes use of a flaw in voice transaction identification mechanisms. Due to the impossibility of physical identification, businesses must rely on other means to identify their customers. These other ways frequently entail demanding confirmation of personal information such as address, date of birth, mother's maiden name, or account number. All of this information is available to the pretexter through social media sites or trash diving.
Pretexting is at the centre of almost every effective social engineering assault, but it has a plethora of definitions, each of which adds to the uncertainty about what it is. Webster's dictionary, for example, describes it as: The act of posing as someone else in order to gain confidential information.

A pretext consists of the subsequent 2 main elements:

A. Plausible State of Affairs:
This is something that would probably result in the target being achieved. It's a sequence of thinkable events, designed and target-hunting by the social engineer to extract data or manipulate the target. The chosen pretext is predicated on the initial intelligence operation. It's this intelligence operation that not solely points to a viable pretext however additionally provides the mandatory data to support it.

B. Character:
The plausible state of affairs involves the social engineer enjoying a “role” very like an associate degree actor. This doesn't essentially mean impersonating somebody real, in fact, it's additional typically a character. However, it's vital to recollect that this square measures several aspects to think about once making a personality. The social engineer should contemplate however they might dress, however they might speak and what reasonable talent set they might have.

2.4 Bating
Baiting is an attack in which a malware-infected storage media is left in a position where the intended victims are likely to find it. It’s just like keeping an alluring item at a location where the victim is bound to come and get attracted. It may be a pen-drive or disk having “Employee salary details” written on it and that is kept near any employee’s desk or any software claiming to give access to thousands of movies. Baiting is a very common technique that is equipped by many attackers to get attention and trap the victim through the different kinds of softwares promising to give free or cost effective services.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 10, October-2021

2.5 Malware and Ransomware

Malware can be easily remembered as MALicious softWARE. Viruses, worms, Trojans, etc. are used in this attack. The malicious software, which rides in a dangerous link or some risky software installation, then attacks the desired software components and starts spreading into other systems.

Ransomware is a step further from Malware, where the attacker demands any amount of money or any work that needs to be done by the victim, after which he brings the computer or device to a stable condition.

2.6 Waterholing

The attack finds the most visited website by his target, finds vulnerabilities in the site and injects malicious code into it. With this the target is redirected to an unknown website or unknowingly downloads some software or code.

3. SOFTWARE VUKNERABILITIES AND ATTACK SURFFACES

The entire number of vulnerabilities that may be used to launch a security assault is referred to as the attack surface. Physical or digital attack surfaces are also possible. The terms attack surface and attack vector are sometimes misunderstood, although they are not interchangeable. The target is the surface, and the vector is the method by which an invader obtains entry. The attack surfaces include:

a. Emails, SMS
b. Online Ads on different websites
c. Social Networking Sites like Facebook, Whatsapp, Instagram
d. Malicious Employees of a particular company who are easily bribed and aren't committed.

Software Vulnerabilities include weak passwords and compromised credentials. They are one of the most discussed entities in any discussion related to Cyber Security, but they aren't given enough importance. Though there are many authentication techniques used now-a-days, passwords and usernames are the most common ones and are implemented easily anywhere. Compromised credentials means a user's credentials, such as usernames and passwords, are exposed to unauthorized entities or are easily guessed by intruders. This typically happens when unsuspecting users fall prey to phishing attempts and enter their login credentials on fake websites. Lost, unexpectedly or unknowingly disclosed credentials are easily exploitable and can be used for malicious activities. Although there are many login systems which make sure that the credentials are not easily guessed, one needs to be responsible. It is not only humans that have access permissions, but architectural components like servers, environments, network devices and security tools often have passwords which are coded and stored. If such codes and passwords are accessed by an intruder, it might cause harm to the whole system and might infect the complete architecture.

4. HUMAN PERSPECTIVE

Humans are one of the weakest, vulnerable and exploitable links in cyber security. Many attacks have been designed keeping in mind how human emotions, nature and behaviour can be manipulated. By evoking strong emotions and exploiting the weaknesses of a particular person, the attacker can easily victimize innocent people and take advantage. Attackers easily exploit emotions like greed, desire, panicking while urgency, etc. for their own benefits. One can refer to the message shown in Figure 2. For instance, a message claiming to give a hundred new mobiles for free can lure many teens as there is always a desire to have an advanced mobile phone and there is also an urgency to get one before the hundred are already ordered by others. One may have come across so many notifications, for an educated and modern person, it might be easily detectable as a scam, but for the common man it might be an opportunity to get something luxurious. This ideology might make him vulnerable to many attacks, which he might not even know after falling to them. The sense of duty can also be exploited. Attackers within a company or from outside send emails to top executives and threaten them of different unwanted consequences to force them to comply with their demands or requests.

Figure 2: A Message triggering a state of urgency inside the mind of victims.

To prevent people from falling into such traps, the ETA method is equipped by most companies and institutes. ETA stands for Education, Training and Architecture. Companies educate their employees about such attacks and how to be safe from these attacks. This whole process is a part of the induction or post-hiring process. In large companies where security of data is a primary issue and all employees might be working with sensitive data, there is specialized training given and assessments conducted on the same. Awareness is being created generally among people and being provided to citizens of all nations. However, the major problem here is that these techniques are really fundamental and basic ones. The seriousness differs at an individual level. Human emotions are more vulnerable and can't be safe-guarded from or by using ML or AI. A computer would deny access to any intruder or the user himself if he forgets the password or inputs wrong passwords, but a human after developing great relations or spending some time with another person tends to trust him or her due to human tendency and is vulnerable to attacks. Only emotionless robots could come closest to securing data. Another problem with Security management and mitigation is that there are some basic rules which all can

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 10, October-2021

follow, but technical knowledge can't be imparted to all and is beyond everyone's scope. More importantly, a silly mistake by any employee from a non-technical background can be fatal for the company and it might be noticed years later.

Now-a-days, the No-Trust Architecture is gaining ground and is being used by many organizations. In this, a company identifies a "Protect Surface". A "Protect Surface" can vary from industry to industry, an automobile company would term protect surface as data regarding the designs and other improvisations of cars, while a technology giant might consider data of users and data regarding the various technical aspects of various softwares as the protect surface. Once identification is done, the administrator identifies the different ways or techniques through which the users, employees, data, infrastructure and other components interact with the "Protect Surface". A micro-perimeter is created with the help of gateways and security checks. This micro-perimeter can give a granular view of who, where, why and how altered the state of the "Protect State". With such minute details, one can easily supervise the traffic and also make required changes in the security checks or measures if required. A segmentation gateway (next generation firewall) can also be equipped to improve the security checks. This will determine who transits through the micro-perimeter and would help in recognizing the unauthorized or malicious user.

5. PREVENTIVE MEASURES

5.1 Spoofed Email Detection:

Email spoofing is impossible to prevent. The only way to detect fake email is to set your spam filtering to detect it. The easiest way to prevent phishing is for the firm to use DMARC (Domain based message Authentication Reporting and conference) to filter fraudulent emails before they reach the client. Because many attackers utilise brand names, they do not trust the email's display name. To create a bogus email, the attacker also employs the spelling mistake approach. Only the "anchor test" is displayed in the web browser in this sort of email, not the URL. The Link Guard algorithm is used to deal with such scenarios. The features of phishing email links produce an algorithm with a set of criteria, such as detecting hyperlinks that are not the same as the actual link.

5.2 Fake Social Network Account Detection:

Many regulations exist on social networking sites to prevent the creation of false profiles, but there is a lack of proper compliance to identify the user. In order to influence someone, this attacker creates a false account. In most cases, the user's personal information is shared in their profile and status. They allow hackers to gather information about individuals in order to execute spear phishing attacks. For example, if a user posts something as basic as "I Love Football," a potential hacker may utilise that information to create a custom spear phishing attack just for that person. To avoid this sort of assault, users should be constantly mindful of what they publish and share, and they should be especially careful of material that they share with others through links.

5.3 Hacking Detection:

It is not easy to detect a hacking assault. Especially for those users who are unaware of account security and are unaware of internet security threats. The most essential thing to remember is to keep your password private. If you give someone your password, you should update it once they've used it. Our personal computers should be free of viruses, keyloggers, and other malware; to do so, we must obtain updated applications, software, and anti-viruses from a reputable source. For their computers and blogs, users must have up-to-date versions of the newest anti-virus software. While surfing the internet, you should be mindful of your surroundings. If you click on a fraudulent link, your email might be compromised. The strength of your password should be such that it cannot be quickly guessed by an adversary. It is extremely critical to maintain the passwords to your banking and other financial accounts safe and hidden. To protect yourself from these sorts of attacks, you should install antivirus software. Antivirus software is essential for keeping your machine in excellent working order. The password should be three-dimensional; it might include numbers, letters, and symbols with a unique personality.

5.4 Trojan Horse Detection:

There are a few things to keep in mind to keep your system safe against Trojan horses.

a) When downloading a file from the internet, be cautious; it's only a matter of time until you become a Trojan horse victim.
b) If a file arrives from a coworker, you must be certain what the file is before releasing it, since many Trojans may try to propagate through a buddy list via an email address book.
c) You should be aware of hidden file extensions; by default, Windows hides a file's final extension. For example, "Susie.jpg" might be "Susie.jpg.exe," which is an executable Trojan, reducing the odds of being duped.

5.5 Water-holing Detection:

Use sequential pattern mining to identify the most visited websites by any user or target. (Something very convoluted, so didn't go deep)

Then a thorough check is conducted on the URLs (internal and external sites) of the website using Link Analysis tools like Link Analysis Pro tool 3.3.37.
For instance:
Phishing url starts with http instead of https

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 10, October-2021

6. ML BASED SOLUTIONS

6.1 SMS Classification:

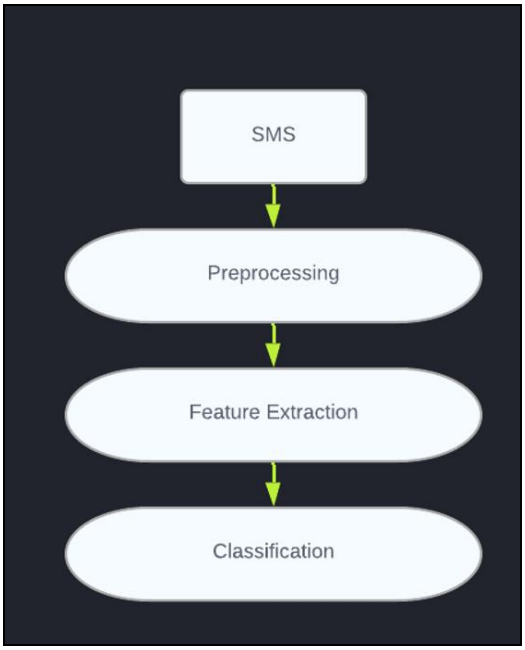

Figure 3: SMS Spam and Ham Classification.

A. Dataset Description:

The Pinterest dataset is utilised to analyse messages, identify differentiating characteristics, and detect smishing messages in this study. Some researchers in the literature treat smishing messages as a subset of spam messages and use other datasets, such as, to identify SMiShing messages. The dataset used in this study comprises 5,574 smishing and genuine mails.

B. Pre-Processing:

Messages are initially preprocessed using appropriate preprocessing methods that are widely employed in text analysis or classification issues before moving on to the feature extraction and classification stages.

- Tokenization is performed to all phrases, allowing tokens (or words) to be deconstructed and processed separately. In most languages, terms like conjunctions and prepositions are called stop words.
- Stop words do not contribute to text discrimination or categorization since they are widely found in most sentences and are independent of the topic. As a result, stop words are no longer used.
- Punctuation marks get deleted.
- Lowercase conversion is done to words to prevent various interpretations of the same term in upper and lower case.
- The root, or stem, forms of the words are derived using the Porter stemming method, which is a popular English stemmer.

C. Feature Extraction:

Following the step of pre-processing. Messages are parsed for several characteristics, which are detailed below.

- Term (Word) Feature: After preprocessing, these characteristics are extracted from the remaining terms, or words, in the sentences. The importance of each phrase in the message is determined by assigning a weight to each term. The frequently utilised Term Frequency - Inverse Document Frequency (TF-IDF) method is employed for this purpose. The number of times a term appears in a document is referred to as term frequency. As a result, it determines how often a phrase appears in a document.The logarithm of the number of documents in the dataset divided by the number of documents where the specified word appears is used to calculate Inverse Document Frequency. As a result, it determines the significance of a phrase.
- URL Feature: One of the most common ways used by attackers to drive their victims to malicious phishing sites or mobile applications is to insert URLs (web page links) into smishing messages. Figure 3 is an example of a smishing message with a malicious URL.
- E-mail Address Characteristic: The inclusion of Email addresses in messages is another significant feature for detecting SMiShing communications. Attackers also utilise this approach to obtain personal information about their victims.
- Phone Number in a Message: The presence of a phone number in a message is also a strong sign of smishing.Attackers use this approach to get confidential information over the phone by persuading their victims to contact a certain phone number. Figure 4 shows an example of a smishing message with a phone number. Messages are represented using multidimensional feature vectors for subsequent processing using the above-mentioned feature types.

D. Classification:

Following the feature extraction stage, the features are input into classification techniques such as Support Vector Machine (SVM), Random Forest (RF), and Logistic Regression (LR) so that messages may be categorised as authentic or smishing.

6.2 Other Applications in AI:

There are potential applications of ai in the fields of dynamic modeling and link prediction. for instance, in dynamic modelling, it is often difficult to predict the intentions of individuals when forming new connections in social networks.

Several prominent researchers have already applied neural networks to model the growth of real world networks. They achieved this by learning from the changes in the data collected by the network as it moves around the world.

The link prediction approaches that were studied by j. kleinberg and d. liben-normant only used mathematical techniques, and only 16% of the predictions were correct.

There have already been neural networks applied to this area. For instance, kimura, saito, and ueda have already developed

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 10, October-2021

networks that can predict new links based on the data collected by the World Wide Web.

Additionally, there has been great use of ML in the fields of intrusion detection in different systems and secured frameworks

7. FUTURE WORK

Future work will involve the development of artificial neural networks or fuzzy systems to detect user behavior in e-mail communication networks. One can also refer the paper to build a SMS classification system and dive deep into ML-based intrusion detection systems.

8. CONCLUSION

This paper highlighted the important techniques of social engineering attacks and also helped in finding some preventive measures for the same. It also emphasized the importance of awareness of social engineering based attacks. Though humans are one of the weakest links in the cyber security domain, various social engineering techniques were discussed through which one can prevent themselves from falling prey to such traps. Also, the meaning of zero trust architecture and the method of implementation was discussed. One of the various architectures and implementation of how ML or AI are used in the domain of cyber security was also discussed.

9. REFERENCES

[1] Ahmad Uways Zulkurnain, Ahmad Kamal Bin Kamarun Hamidy, Affandi Bin Husain, Hassan Chizari.: "Social Engineering Attack Mitigation". International Journal of Mathematics and Computational Science Vol 1 (4), 188–199 (2015).

[2] Surbhi Gupta, Abhishek Singhal, Akanksha Kapoor: "A Literature Survey on Social Engineering Attacks: Phishing Attack". ICCCA (2016).

[3] A. Saravanani and S.Sathya Bama: "A Review on Cyber Security and the Fifth Generation Cyberattacks". Oriental Journal of Computer Science and Technology Vol. 12 (2), 50-56 (2019).

[4] Aviral Sangal, Dr. Harsh Kumar Verma: "A Static Feature Selection-based Android Malware Detection Using Machine Learning Techniques". International Conference on Smart Electronics and Communication (ICOSEC 2020)

[5] Abeer Alotaibi, Emad S Alsuwat: "A Study on Socila Engineering Attacks : Phishing Attacks", International Journal of Recent Advances in Physics (2021)

[6] T. Subburaj, K. Suthendran: "Digital Watering Hole Attack Detection Using Sequential Pattern".

[7] Sandhya Mishra, Devpriya Soni: "SMS Phishing and Mitigation Approaches". IEEE (2019)

[8] Sriendra Deshan Ilangakoon, Abeywardena K.Y: "The Use of Subliminal and Supraliminal Messages in Phishing and Spear Phishing based Social Engineering Attacks; Feasibility Study". The 13th International Conference on Computer Science & Education (ICCSE 2018)

[9] Fatima Salahdine, Naima Kaabouch: "Social Engineering Attacks: A Survey", School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks.

[10] Devika C.J Nair, Teslin Jacob.: "AN AUTOMATED SYSTEM FOR DETECTION OF SOCIAL ENGINEERING PHISHING ATTACKS USING MACHINE LEARNING". International Journal of Engineering and Technology Vol 7 (7), (2020).

[11] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl: "Advance Social Engineering Attacks". Journal of Information Security and Applications (2014)

[12] Rupali Patil, Nishant Gada, Krisha Gala: "Twitter Data Visualization and Sentiment Analysis of Article 370".

[13] Robert Luo, Richard Brody, Stephen Burd, Alessandro Seazzu: "Social Engineering: The Neglected Human Factor for Information Security Management". Information Resources Management Journal July-September 2011

[14] ZUOGUANG WANG , HONGSONG ZHU, LIMIN SUN: "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods"

[15] Usman Shuaibu Musa , Megha Chhabra, Aniso Ali , Mandeep Kaur: "Intrusion Detection System using Machine Learning Techniques: A Review"

[16] Mark Jyn-Huey Lim, Michael Negnevitsky, Jacky Hartnett: "Artificial Intelligence Applications for Analysis of E-mail Communication activities".