International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks

[*1]Shaista Sayeed, [2]Indu Cherupally, [3]Narmada Muthyala

[1]Assistant Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

[2,3]Students, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 10 April 2023
Published: 30 April 2023

Publication Issue
Volume 9, Issue 2
March-April-2023

Page Number
672-676

ABSTRACT

Despite Emails and websites being widely used for communication, collaboration, and day-to-day activity, not all online users have the same knowledge and skills when determining the credibility of visited websites and email content. As a result, phishing, an identity theft cyber-attack that targets humans rather than computers, was born to harvest internet users' confidential information by taking advantage of human behavior and hurting an organization's continuity, reputation, and credibility. Because the success of phishing attacks depends on human behavior, using the Health-Belief Model, the study's objective is to examine significant factors that influence online users' security behavior in the context of Email and website-based phishing attacks. The model included eight predictor variables and was validated using quantitative data from 138 academic staff. The study findings exhibit that 4 out of 8 predictor variables, namely Perceived-Barriers, Perceived-Susceptibility, Self-efficacy, and Security-Awareness, are statistically significant in determining users' security behavior. The study's outcome is to assist in the appropriate design of both online and offline content for cyber security awareness programs, focusing on Email and website-based phishing attacks.

Keywords: Confidential Data, Health Belief Model, Online User, Phishing Attack, Security Behavior.

I. INTRODUCTION

The Internet has revolutionized individuals' and organizations' communication, collaboration, and day-to-day activity. Despite its multifaceted benefits, heavy reliance on the Internet has introduced various security challenges. Due to professional hackers are now aware that online users are becoming the weakest link in cyberspace, "Only amateurs attack machines; professionals target people" (Schneier, 2000). Phishing is a modern-day identity theft cyberattack that targets humans rather than the computer system (Kathrine, Praise, Rose & Kalaivani 2019). Phishers leverage human behavior to capture personal information from online users via Email, websites, SMS, and social media. It deceives naive users and IT experts because attackers

always follow novel strategies (PhishLabs, 2019; Kathrine et al., 2019). Despite technology-based solutions such as phishing filters and popup blockers assisting online users in spotting fake websites and emails (Frauenstein, 2014), online users lack what security indicators signify; they ignore browser security warning alerts for monetary rewards (Kirlappos and Sasse, 2012), they do not want security warning alerts to disrupt their online activities, so they just focus on the areas of their interest that are most important to them (Krol,Moroz & Sasse 2012). The spelling errors in the URL structures, such as "g00gle.com" and "google.com", "twitteer.com" and "twitter.com," may go unnoticed by online users. The cybercriminal uses this advantage to design and send the exact duplicates of legitimate websites. Afterward, fraudulent websites collect confidential information from unnoticed online users, potentially resulting in login credential compromise, data loss, and financial loss. The phishing attack lifecycle concepts presented in Figure 1 were taken from (Baadel & Lu, 2019; Patil & Dhage, 2019), with some modifications for our study. Anti-phishing interventions at any step in Figure 1 could avert Email and website-based phishing attacks.

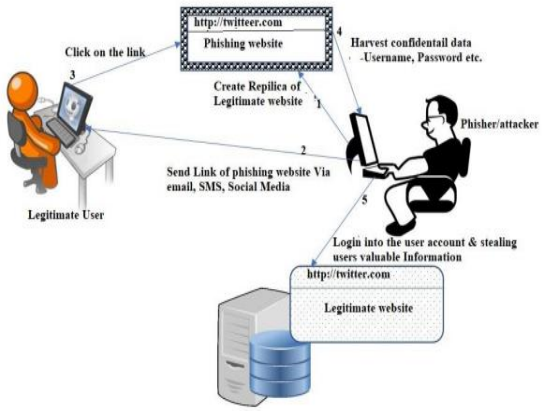

Figure 1: Example of Phishing Attack Life Cycles

Successful phishing attempts could result in catastrophic data loss, login credential compromise, ransomware infection, and financial loss (Proofpoint, 2020). Encryption ransomware was found in 93 % of all phishing emails (PhishMe, 2016). Unless a ransom is paid, internet users will be denied access to their data. Despite security awareness programs and phishing simulators, online users are still vulnerable to phishing emails (Williams, Hinds, & Joinson, 2018). Fake lottery or prize advertisements; impersonation or identity theft; computer or Internet faults; and promising big money in return) were among the main reasons for online users being exposed to phishing scams or fraud (EUC, 2020). Existing technological defenses will be ineffective against someone who does not follow acceptable Information security policies and procedures. Although training is beneficial, it will never be entirely successful (Pharris, 2019). Because the security of an organization's and online users' information cannot be ignored, technological protection alone has been proven to be insufficient to protect online users' sensitive information; this study is proposed to examine significant factors that influence online users' security behavior in the context of Email and website-based phishing attacks using well known behavioral model i.e., Health Belief Model (HBM).

II. RELATED WORK

In addition to predicting patients' compliance with acceptable healthcare behavior, HBM was used in determining: Email related users' security behavior (Ng et al., 2009), home computer users' security behavior (Claar, 2011; Edwards, 2015), employee's security behavior intentions at workplace (Williams et al., 2014), and in determining impacts of security awareness on employee's security behavior (Li. et al. 2016). Despite the relevance of the studies above' findings, examining significant factors that influence online users' security behavior in the context of both Email and website-based phishing attacks was not a significant focus of these studies. Since successful phishing attempts can result in catastrophic data loss, login credential compromise, ransomware infection, and financial loss (Proofpoint, 2020), addressing the gaps mentioned above in this study is a vital step. Ng et al. (2009) used the HBM to investigate employees' email security behavior. They found that perceived susceptibility, perceived benefits, and self-efficacy are

statistically significant in determining users' email security behavior. Claar (2011) used the HBM to investigate home computer users' security behavior and found that perceived susceptibility, Severity, barriers, and self-efficacy are statistically significant in determining home computer users' security behavior. Perceived Susceptibility, Benefits, Severity, and Cues to Action were statistically significant in affecting users' security behavior intentions, according to Williams et al. (2014). Edwards (2015) used HBM to determine an association between security awareness and home computer users' security behavior and found that Perceived Susceptibility and privacy concerns are statistically significant in determining Home computer users' security behaviors. Li., et al. (2016) used HBM along with Protection Motivation Theory (PMT) to examine the impacts of security awareness on employees' security behavior and found that Perceivedsusceptibility, Self-Efficacy, Perceived-severity, and response efficacy are statistically significant in determining employees' security behaviors. However, the research findings demonstrated in the studies mentioned above are found to be inconsistent. Perceived Benefit is statistically significant in determining users' security behavior in the study (Ng, et al., 2009; Williams et al., 2014), while it is not statistically significant in the study (Claar, 2011; Edwards, 2015). In the study (Ng et al., 2009; Claar, 2011; Li. et al., 2016), Self-Efficacy is statistically significant in determining users' security behavior, while it is not statistically significant in the study (Williams et al., 2014; Edwards, 2015). In the study (Claar, 2011), Perceived barriers are statistically significant in determining users' security behavior, while it is not statistically significant in the study (Ng et al., 2009; Williams et al., 2014; Edwards, 2015, Li et al., 2016). Cues-To-Action is statistically significant in determining users' security behavior in the study (Williams et al., 2014), while it is not statistically significant in the study (Ng et al., 2009; Claar, 2011; Edwards, 2015; Li. et al., 2016). Edwards (2015) added two new constructs to HBM: security awareness and privacy concern, and found that security awareness is not statistically significant in determining users' security behavior, while privacy concern is. Therefore, this study balances the inconsistent research findings of previous studies by conducting both theoretical and empirical validation and filling research gaps in connection to Email and website-based security practices in the context of phishing attacks.

III. PROPOSED SYSTEM

The research method used here is based on the empirical research and also uses the literature review. Where the usage of the world wide web given a statistics that the online marketing has been increased a now a days by social media users. The Research questions :

- Why we need use the social media for marketing?
- How the companies analyse the sales criteria in social media?

1. Low cast marketing

The efforts taken to market a product is not that expensive, and moreover within the less amount of time it can reach vast category of people. The maintenance of the marketing is easy compared to other methods. The company gets more exposure of its products.

2 .Customer relationship

As customer use social media often or daily bases. The interest of the customer is gathered through some techniques for example in Facebook liking the page and sharing and commenting positive feedbacks about the product makes greater impact for the company. It is easier for them to see and interact with the marketing websites and make the decision quickly.

3. Advertisement

Instead of advertising their products only in their website or many of the websites it will be a beautiful idea to advertise their product through social media.

4. Social activities

Social activities are done on media such as Facebook, LinkedIn, twitter and many more application that makes them to see the products and they can show their interest of the product. Where, most of the customer relaxes and can see the advertisement and make the plans according to their wish on the go.

5. Attractive offers

Customers buy products mainly because of attractive offers that the companies shows during the time interval and the purchase price is low compared to the normal purchase.

6. Sales

All the factors about will definitely lead the company to the greater sales results. Where they could analyse the sales record and maintain their business in the higher rank by adding positive feedbacks from customers.

User behaviour on social media is carefully watched by using personalization algorithms there they could filter the interest and preferences of the each and every individual. We cannot believe that the companies are always transparent. So accessing SNS (Social networking sites) may affect the privacy of the customer as well.

1. Clicking the links

When the user saw the advertisement on social media they click the link to see the website. Here the activities of the user is been analysed by the company. Such as the purchase category or the item they are interested to buy are monitored and filtered. Sometime the link will activate other type of advertisements where the customer must see at least for 1 minute.

2. Searching

Searching on google for a specific information is stored in the database of the server. The location, gender, culture, native language, time sent on SNS and the behaviour when they navigate through that website will be thoroughly seen and based on that the record of each and every customer details are stored.

3. Reflection in social media

When the customer makes purchase using social media, the behaviour of the user is keenly watched by the companies, for example if they like the page or says something good about the company or tweets about the website or recommending our friend to buy etc., makes a great change for the companies. And they would continuously sending the offers, advertisements by messages or emails.

4. Privacy threats

It makes the storage and selling and use of privacy information without the awareness of the user. These actions can result in personal privacy damage. Companies collect information of people to target the product and built their business needs. This leads to illegal or unethical acquisition of information, storage and selling. For example they collect information like address, email id, accessing newsgroup are collected and handed over to the third parties. In which the threats of misusing the information is not predicted.

5. Payment

In the digital environment the payment becomes online like credit, debit or check which traces the behavior of the customer. Where, digital signature should be maintained in order to map the identity of the user with their bank. Chips can be inserted to the smart card thereby misusing or hacking the data is minimized.

IV. CONCLUSION

Social media widely used for companies to improve their business by accessing the personal information and uses technologies to gather information, analyses it and use that information for the growth of the company. Monitoring the behaviour of the user should not go beyond the privacy protection policy. User believes the website that they can use the social media for the benefit of their need. So the violation of the usage of the social networks should not be done. These websites should maintain the privacy policy. Which makes both customer and the business people get profit,

the customer must satisfy by buying the product thereby marketing should also be improved.

V. REFERENCES

[1]. Composite Behavioral Modeling for IdentityTheft Detection in Online Social NetworksCheng Wang, Senior Member, IEEE, and Bo Yang

[2]. The Continuous Rise for Social Networking Privacy and Security, Adrian M. Powell Professor Li Yang CPSC 5620, Computer Network Security University of Tennessee at Chattanooga April 20, 2012

[3]. Social networking and identity theft in the digitalSocietyEric HolmBond University, eric.holm@student.bond.edu.au

[4]. Business Growth thru Social Media Marketing, AbeerAlharbie,College of Public and International Affairs,University of Bridgeport, Bridgeport, CT06604, USA

[5]. Quaestus multidisciplinary research journalthe growing importance of social mediaIn business marketing Pavel Ciprian

[6]. Awareness of Behavioral Tracking and InformationPrivacy Concern in Facebook andGoogleEmilee RaderDepartment of Media and InformationCollege of Communication Arts and SciencesMichigan State Universityemilee@msu.edu

[7]. The Impact of Social Media on Business Growth andPerformance in IndiaITina P. Singh, IIDr.RatnaSinhaIResearch Scholar, ISBR Research Centre, Mysore University, Karnataka, IndiaIIResearch Guide, ISBR Research Centre, Mysore University, Karnataka, India

[8]. Developing an Internet Marketing Strategy 2011 The Internet Marketing Academy &Ventus Publishing ApSISBN 978-87-7681-813-5.

[9]. “IntSocial Media, How does it Work for Business?”,W. V.Siricharoen, Member, IACSITernational Journal of Innovation, Management and Technology, Vol. 3, No. 4, August 2012

[10]. International Journal of Enterprise Computing and Business System, “Social media and its role in Marketing”,Ms.SisiraNeti, ISSN: 2230-8849, July 2011

Cite this article as :

Shaista Sayeed, Indu Cherupally, Narmada Muthyala, "Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.672-676, March-April-2023.