State of Research on User Psychology involved in Phishing Attacks

Aniket Bhadane
Corresponding author : College of Engineering Pune
Email : aniketbhadane93@gmail.com

Sunil B. Mane
College of Engineering Pune
Email : sunilbmane@gmail.com

We present a survey of literature on User Psychology involved in Phishing attacks. Phishing messages and websites masquerade as a trusted source and continue to be a problem for corporates and individuals causing huge tangible and intangible losses. Phishing is a wide-spanning attack and cannot be solved in one single way. It requires a collaborative effort in all directions. Solutions to mitigate phishing are mainly detecting the attack using automated software techniques, training users, and designing better interfaces to guide users in taking informed decision. It is important to understand end-user psychology which is exploited by social engineering techniques used in these attacks, to build effective countermeasures. Phishing is constantly on rise with current trends showing huge increase in Spear Phishing attacks and Social Media-based attacks.

Keywords: Phishing, Social Engineering, Usable Security, Human Computer Interaction, User Characteristics

1. Introduction

Phishing attacks masquerade as a trustworthy source, often spread using socially engineered messages using media such as emails, social media, SMS, online multiplayer games, VoIP, etc. to persuade victims to perform certain actions of attacker's benefit [1]. These actions can be persuading the user to enter sensitive information on a phishing website; clicking a malicious/ phishing link in an email; performing certain actions, such as money transfer, installing malicious software etc., as stated in the socially engineered message. Social engineering is psychological manipulation of people to make them perform certain actions [2].

Phishing attacks caused loss of over $3 Billion in last 3 years [3] and have seen an increase of 65% in 2016 over 2015 [4]. Spear Phishing attacks constituted 90% of all phishing attacks. A Spear phishing attack costs $1.6 Million on average, and $3.7 Million is spent a year by an average 10,000-employee company dealing with phishing attacks [5]. Very recent major phishing incidents include phishing attempts after Equifax data breach, the Google Docs phishing attack and the DNC hack. Phishing emails and websites were found masquerading as Equifax after its massive data breach [6][7]. In the Google Docs phishing scam, almost 1 million Gmail users were affected [8]. And the DNC hack [9] led to the leak of 19,252 emails and 8,034 attachments from the DNC, the governing body of the United States' Democratic Party.

The past work on phishing can be categorized into four categories: understanding why people fall for phishing, automated software techniques to detect phishing, training people to not fall for phishing attacks, and better user interfaces to help people make better decisions when confronted with an attack [10].

We provide an ordered study of the current state of research on User Psychology involved in phishing, so that effective counter-measures can be developed. This understanding can be used in designing better User Training programs and User Interfaces. We do not cover related topics in details, such as spam, but we do touch upon such points wherever required.

Section 2 describes human psychology involved in phishing. In Section 3, we provide the learnings of our study and their uses in designing better training programs and user interfaces. Lastly, we conclude in Section 4.

2. Phishing Psychology

A semantic attack like phishing exploits human vulnerabilities. Before knowing what anti phishing techniques have been developed, it is essential to know the human factors such as why users fall for phishing, demographics, etc. involved in phishing, to understand what countermeasures need to be taken. It is necessary to have detailed understanding of users' motivations and perspective of the system, in order to build strong countermeasures.

Phishing messages generally use sentiments and psychological principles of influence authority, scarcity, curiosity, fear, urgency, social proof etc [11].

An early study by Dhamija et al. [12] found that even experienced users can fall prey to visual deception attacks. Good phishing websites fool most of the users. Their results show that the standard security indicators and cues are not effective for a large fraction of users and did not help in preventing users from falling victim to phishing attacks. The study by Wu et al. [13] also backed these findings. Dhamija et al. also mentioned five types of users based on strategies users used to classify whether a site was legitimate or not.

Khonji et al. [1] state that

Table 1 : Hypothesis on Facebook Habits and their Results as per Vishwanath [20]

Hypothesis	Result
Higher habitual facebook users are more likely to frequently use facebook	Proved
Higher habitual facebook users are more likely to have large social network of friends on facebook	Proved
Higher habitual facebook users are more likely to be deficient in their ability to regulate their social media use	Proved
Higher habitual facebook users are more likely to fall victim to level1 and 2 attacks	Proved
Higher attitudinal commitment users are more likely to fall victim to Level1 and Level2 attacks	Level1 Proved, Level2 Not Proved
Users with higher level concern for online privacy are less likely to fall victim to Level1 and Level2 attacks	Level1 Proved, Level2 Not Proved

employees' use of computers in places other than corporate environment where IT infrastructure exists, can make people imbibe habits such as disregarding security indicators and warnings, and people can carry those habits at workplaces too.

Downs et al. [14] found that even though people have awareness of phishing, they cannot effectively use this awareness to identify phishing attacks. In another study [15], they showed that users' awareness of negative consequences did not contribute much in reducing their susceptibility to attacks.

According to Gonzalez and Locasto [16], the main components of phishing attacks are: psychology, computation, and sociology. They mention that study of interdisciplinary fields is important to understand social engineering attacks, so that the psychological and sociological vulnerabilities exploited in attacks can be better understood.

Canfield et al. [17] conducted experiments to find performance of users in Detection deciding whether a mail is phishing or not, and Behavior deciding what action to take on a mail. With the help of signal detection theory, they show that phishing-related decisions are sensitive to users' confidence and view on consequences.

Wang et al. [18] state that prior studies have overstressed on prospective overconfidence (people's beliefs about their capabilities) in phishing detection ability of users, but retrospective overconfidence (judgmental confidence) has more effect on users' behaviors.

Conway et al. [19] conducted interviews, with the help of cognitive psychology, with employees from a financial services institution on their experiences of Phishing. They found that the variation in workload and the number of unimportant mails that an employee interacts with on a daily basis, have relations with phishing susceptibility. They also found that employees had more secure feeling within the IT infrastructure of the company, which may make their behavior less cautious. Additionally, people with low beliefs of their technical capabilities had lesser willingness to share their experience of victimization with peers.

Older studies such as Sheng et al. [21] found age and gender to be leading demographics that predict phishing susceptibility. Women were found to be more susceptible to phishing than men, mainly due to lesser exposure to technical whereabouts. Younger users in ages 18 to 25 had worst performance among all age groups, mostly due to lesser risk aversion. Sheng et al. considered middle-aged, and not older (60 years and older) Internet users. A study in 2017 by Oliveira et al. [11] included older adults (65 years and older). They created fake spear phishing emails considering Principles of Influence (called Weapons of Influence in the paper) and Life Domains. They also provide examples of different types of messages they used for spear phishing. Data collection took place at the participants' homes to increase ecological validity. From prior literature, they mention that general cognitive processing capacities and sensitivity to deception decline with age, and scamming is most effective in older adults. Their research findings show that younger users were found to be most susceptible to scarcity (e.g.: "once in a lifetime opportunity" type messages), while older users were most susceptible to reciprocation (e.g.: luring user to install malware by offering a free gift).

Vishwanath [20] studied users' Facebook usage habits and their relation with user susceptibility to social media phishing attacks. He categorizes attacks as: Level1 attack friend request, Level2 attack information-request. He mentions six hypotheses and tests them. This is shown in Table 1. The results show that habitual facebook use, resulting in automaticity of response is a leading factor involved in an individual's victimization in social media attacks.

Summarizing, people of different demographics have different psychological vulnerabilities. People have different habits and perceptions in different environments, with habituation playing a major role in user susceptibility to social media phishing attacks. Users' confidence and their view on consequences are also involved in users' susceptibility to phishing attacks.

3. Discussion

We discussed about state of research of on User Psychology involved in Phishing Attacks. Phishing attacks have shown to be evolving over time, and continue to be a threat to corporates and individuals. Phishing cannot be dealt in one specific way, but requires a collaborative effort in all directions.

3.1 Social Psychology

It is important to understand human psychological factors leading to phishing victimization, such as confidence, perception of

consequences, habits, automaticity, attentional models, etc. Users of different demographics can be studied to understand which demographics play major role in success of phishing attacks today. It is necessary to have detailed understanding of users' psychological factors involved in phishing, to build strong countermeasures. Factors such as ecological validity need to be considered when designing such studies.

3.2 Use in designing User Training Programs

Use of psychological factors and demographics can help in designing user training approaches for phishing detection. Interdisciplinary fields such as Learning Sciences, Cognitive Sciences and Educational Psychology can prove to be helpful in designing training approaches for enabling retention of knowledge learned in training and its application at the time of attack. Instead of only giving knowledge about these attacks to users, it is also important to teach them how to deal with these attacks in real time. And training users at the time of the attack has been found to be the most effective way of training users. The best way of training against phishing attacks is "at the moment of attack periodic demographic tailored" training.

3.3 Use in designing User Interfaces

When a user is confronted with an attack, if proper indicators are shown to him at that time, it can guide him to take better informed decisions. Lack of effectiveness of security indicators also plays a major role in why users take wrong decisions when dealing with phishing attacks. Using the principles of Human Computer Interaction and Warning Sciences can help in designing such interfaces.

4. Conclusion

In this paper, we provided details on different aspects of User Psychology involved in phishing. Phishing remains to be a major security threat for the corporates and for the general internet users. Phishing is not limited to a single communication media, and spans across different types of media such as Emails, Social Media, online multiplayer games, etc. We provide an organized study covering aspects of User Psychology to build effective counter-measures against phishing. Phishing, being a multifaceted attack, requires research to be done in all aspects. Technical solutions to mitigate phishing are not 100% effective and some attacks do reach the end users. Hence, it is important to research on developing better training programs and user interfaces, with the help of understanding users' psychology. Moreover, phishing attacks, especially Spear Phishing attacks, continue to become more sophisticated and cause loss of billions of dollars and also intangible loss such as damaged brand reputation. To build effective countermeasures, it is important to understand the psychology of users which makes them fall for phishing attacks. It is important to secure all doors to not allow phishers to conduct such attacks.

Acknowledgement

The authors would like to thank anonymous reviewers for their valuable comments.

References

[1] M. Khonji, Y. Iraqi, A. Jones, Phishing Detection: A Literature Survey, IEEE Communications Surveys Tutorials 15 (4) (2013) 2091–2121. doi: 10.1109/SURV.2013.032213.00009.

[2] Social engineering (security), page Version ID: 800193757 (Sep. 2017). URL https://en.wikipedia.org/w/index.php?title= Social engineering (security)

[3] Internet Crime Complaint Center (IC3) | Business E-mail Compromise: The 3.1 Billion Dollar Scam (2016). URL https://www.ic3.gov/media/2016/160614.aspx

[4] apwg trends report q4 2016.pdf (2017). URL http://docs.apwg.org/reports/apwg trends report q4 2016.pdf

[5] J. Crowe, Phishing by the Numbers: Must-Know Phishing Statistics 2016 (2016). URL https://blog.barkly.com/phishing-statistics-2016

[6] Equifax or Equiphish? — Krebs on Security (2017). URL https://krebsonsecurity.com/2017/09/equifax-or-equiphish/

[7] After Massive Data Breach, Equifax Directed Customers To Fake Site (2017). URL http://www.npr.org/sections/thetwo-way/2017/09/21/ 552681357/after-massive-data-breach-equifax-directed- customers-to-fake-site

[8] A. Robertson, Google Docs users hit with sophisticated phishing attack (May 2017). URL https://www.theverge.com/2017/5/3/15534768/google-docs-phishing-attack-share-this-document-with-you-spam

[9] How hackers broke into John Podesta, DNC Gmail accounts – Naked Security (2016). URL https://nakedsecurity.sophos.com/2016/10/25/how-hackers- broke-into-john-podesta-dnc-gmail-accounts/

[10] Y. Zhang, J. I. Hong, L. F. Cranor, Cantina: A Content-based Approach to Detecting Phishing Web Sites, in: Proceedings of the 16th International Conference on World Wide Web, WWW '07, ACM, New York, NY, USA, 2007, pp. 639–648. doi:10.1145/1242572.1242659. URL http://doi.acm.org/10.1145/1242572.1242659

[11] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, N. Ebner, Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing, in: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17, ACM, New York, NY, USA, 2017, pp. 6412–6424. doi:10.1145/3025453.3025831. URL http://doi.acm.org/10.1145/3025453.3025831

[12] R. Dhamija, J. D. Tygar, M. Hearst, Why Phishing Works, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '06, ACM, New York, NY, USA, 2006, pp. 581–590. doi:10.1145/1124772.1124861. URL http://doi.acm.org/10.1145/1124772.1124861

[13] M. Wu, R. C. Miller, S. L. Garfinkel, Do Security Toolbars Actually Prevent Phishing Attacks?, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '06, ACM, New York, NY, USA, 2006, pp. 601–610. doi:10.1145/1124772.1124863. URL http://doi.acm.org/10.1145/1124772. 1124863

[14] J. S. Downs, M. B. Holbrook, L. F. Cranor, Decision Strategies and Suscep- tibility to Phishing, in: Proceedings of the Second Symposium on Usable Privacy and Security, SOUPS '06, ACM, New York, NY, USA, 2006, pp. 79–90. doi:10.1145/1143120.1143131. URL http://doi.acm.org/10.1145/1143120. 1143131

[15] J. S. Downs, M. Holbrook, L. F. Cranor, Behavioral Response to Phishing Risk, in: Proceedings of the Anti-phishing Working Groups 2Nd Annual eCrime Researchers Summit, eCrime '07, ACM, New York, NY, USA, 2007, pp. 37–44. doi:10.1145/1299015.1299019. URL http://doi.acm.org/10.1145/1299015. 1299019

[16] R. Gonzalez, M. E. Locasto, An interdiscplinary study of phishing and spear-phishing attacks. URL http://cups.cs.cmu.edu/soups/2015/papers/eduGonzales.pdf

[17] C. I. Canfield, B. Fischhoff, A. Davis, Quantifying Phishing Susceptibility for Detection and Behavior Decisions, Human Factors 58 (8) (2016) 1158– 1172. doi:10.1177/0018720816665025. URL https://doi.org/10.1177/001872081 6665025

[18] J. Wang, Y. Li, H. R. Rao, Overconfidence in Phishing Email Detection, Journal of the Association for Information Systems 17 (11). URL http://aisel.aisnet.org/jais/vol17/iss11/1

[19] D. Conway, R. Taib, M. Harris, K. Yu, S. Berkovsky, F. Chen, A Qualita- tive Investigation of Bank Employee Experiences of Information Security and Phishing, in: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association, 2017, pp. 115–129. URL https://www.usenix.

Contd. on page 39

```
>>>
150
>>>
```

Fig. 13 : Output of Program Listing 5

Implementing Files in Python

File data structure stores the records permanently. Various types of file organization includes sequential file organization, direct access file organization and indexed file organization.

In sequential files records are stored sequentially. The records are also accessed from file sequentially. In direct access files we can write a record to particular position and record can be assessed directly by record number. There exist some relation between the record key and record address.

In Indexed file organization records are stored in sequential file which is main file. A primary key with its offset is stored in index file. When we want to search a given record, first it is searched in index file. From index file, we can get exact location of that record in the sequential file. The sample Python code for writing data to text file and displaying contents from file is given in Fig.14 and output of the same in displayed in Fig.15.

```
fp = open("Input.txt", "w")
fp.write("Department of Information
Technology, Amrutvahini College of
Engineering, Sangamner, Ahmednagar,
Maharashtra")
fp.close()
# Read a file
fp = open("Input.txt", "r")
Message = fp.read()
fp.close()
print Message
```

Fig. 14 : Program Listing 6

```
Department of Information Technology,
Amrutvahini College of Engineering,
Sangamner, Ahmednagar, Maharashtra
```

Fig. 15 : Output of Program Listing 6

Concluding Remarks

As elaborated with few examples, handling the data structures is very easy in Python with minimum lines of code. As Python is platform independent, same Python code can be executed on multiple platforms. Because of its multiple special features, Python is becoming popular and widely used in applications such as developing desktop graphical user interfaces (GUI), software development, education purpose, web based and internet development, scientific and numeric and business applications. ■

About the Author

Dr. Baisa L. Gunjal [CSI Membership: CSI-N1111399] has completed PhD, Computer Engineering from Savitibai Phule Pune University and presently working as professor and head, Information Technology Department, Amrutvahini College of Engineering, Sangamner, MS,India. She has published more than 28 research articles at international and national levels and having more than 386 google scholar citations on her credit. She is recipient of 'Best Teacher Award-2013' from 'Savitribai Phule Pune University,' 'Lady Engineer Award-2012' from 'Institution of Engineers', 'Active Faculty Award for Women-2012', 'Maximum Publications in CSI Award-2013' and "Yasho-Kirti Award 2017" from 'Computer Society of India', 'Best Research Paper award' in international conference INDICON-2014. She can be researched at hello_baisal@yahoo.com.

Contd. from page 36

org/system/files/conference/soups2017/soups2017-conway.pdf

[20] A. Vishwanath, Habitual Facebook use and its impact on getting deceived on social media, Journal of Computer-Mediated Communication 20 (1) (2015) 83–98. URL http://onlinelibrary.wiley.com/doi/10.1111/jcc4.12100/full

[21] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, J. Downs, Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, ACM, New York, NY, USA, 2010, pp. 373–382. doi:10.1145/1753326.1753383. URL http://doi.acm.org/10.1145/1753326. 1753383

■

About the Authors

Aniket Bhadane received his Bachelor of Engineering (Computer) degree from Savitribai Phule Pune University (formerly University of Pune) in 2015. He is currently pursuing M.Tech. Computer Engineering degree from College of Engineering Pune (COEP). His research interests are in the field of cyber security, user authentication and usable security.

Dr. Sunil B. Mane (Membership No. 1096269) is working as Associate Professor, Department of Computer Engineering and Information Technology, College of Engg., Pune (An Autonomous Institute of Govt. of Maharashtra). He has more than 15 years of teaching experience. Dr. Mane has over 25 research publications in various national/international journals and conferences. He is a Board of Studies member in Computer Engineering/Information Technology of various autonomous engineering institutes. He delivered lectures on information and cyber security domain as invited speaker. He is serving as Co-Chief Investigator for the Information Security Education and Awareness (ISEA) project, Ministry of IT, Govt. of India. His area of research is data privacy and cyber security.