Poster: Understanding User's Decision to Interact with Potential Phishing Posts on Facebook using a Vignette Study

Sovantharith Seng
sovantharith.seng@mail.rit.edu
Rochester Institute of Technology
Rochester, New York

Huzeyfe Kocabas
huzeyfe.kocabas@aggiemail.usu.edu
Utah State University
Logan, Utah

Mahdi Nasrullah Al-Ameen
mahdi.al-ameen@usu.edu
Utah State University
Logan, Utah

Matthew Wright
matthew.wright@rit.edu
Rochester Institute of Technology
Rochester, New York

Abstract

Facebook remains the largest social media platform on the Internet with over one billion active monthly users. A variety of personal and sensitive data is shared on the platform, which makes it a prime target for attackers. Increasingly, we see phishing attacks that take advantage of users' lack of security knowledge, deceiving victims by using fake or compromised accounts to share malicious posts. These attacks may slip undetected by the Facebook defense system, exposing users to potentially be phished or have their devices infected with drive-by downloads and malware. Only a few studies have been conducted to date to understand how users interact with attacks like this in Facebook. In our prior work, we conducted a study to address this challenge using a simulated interface and think-aloud protocol. In this study, we aim to make further progress in understanding the impact of different factors on users' clicking decision in social media through a vignette study that encourages participants to think about realistic scenarios that they might face.

CCS Concepts

• **Security and privacy → Social network security and privacy**; *Social aspects of security and privacy*.

Keywords

social media; facebook; phishing; vignette study

ACM Reference Format:
Sovantharith Seng, Huzeyfe Kocabas, Mahdi Nasrullah Al-Ameen, and Matthew Wright. 2019. Poster: Understanding User's Decision to Interact with Potential Phishing Posts on Facebook using a Vignette Study. In *2019 ACM SIGSAC Conference on Computer& Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3319535.3363270

CCS '19, November 11–15, 2019, London, United Kingdom

ACM ISBN 978-1-4503-6747-9/19/11.
https://doi.org/10.1145/3319535.3363270

1 Introduction

Social media platforms like Facebook have become an integral part of life for billions of people. Unfortunately, many users lack the awareness and skills to use these sites securely [3, 5, 13]. Recently, there has been an increase in phishing attacks on social media sites using fake or compromised accounts [4, 9, 10]. In social media, attackers can improve their chance of getting users to click on the links through targeted attacks that exploit the personal information that users share on the site. Although a targeted attack requires more time and effort, it can be more successful and harder to detect both by current defense systems [15] and by users.

To date, there has been a little research aimed to understand the efficacy of attackers' strategies in carrying out phishing attacks in social media, which is important to investigate for improving both defense mechanisms and user awareness. This study extends upon our previous work [12] on this research goal. Our prior work used an interface prototype for an in-person lab study with a think-aloud protocol to understand users' clicking behavior, where the prototype resembles the Facebook newsfeed interface. The interface had details such as post author's profile picture and the post preview details replaced with placeholders to remove personal bias. The post author's name was also replaced with a label of the relationship between the user and the post author (e.g. "close friend"). In this way, we created an artificial Facebook interface for a study in a controlled setting.

The study we now report on in this paper is motivated in part by the feedback that we received on the previous work concerning the artificiality and unfamiliarity of the simulated interface used for the study. To this end, we used a *vignette study*, in which we presented participants with verbal details and asked them to use their imagination to create the corresponding scenario in their mind. Using these vignettes also allowed us to explore more scenarios than our prior work [12], contributing to a deeper understanding of users' clicking behavior in social media.

2 Related Work: Phishing in Social Media

Phishing in email has a very low rate of success, with just 3% of users clicking on links for emails that make it to their inbox [14]. In social media, however, 25% of users click on malicious links [8]. This raises the question of why the success rates of attacks are so high in social media. Alam et al. [1] noted that the success of

targeted phishing is correlated with the amount of information the attacker has. Therefore, if an attacker can become a friend with the victim or uses a compromised account of a friend of the victim, he will have little difficulty in fooling the victim without getting noticed. Social media users expose a lot of personal information through the site, particularly to their connections, so this likely aids attackers.

Another reason that the attacks are successful is due to how Facebook is used. Joinson [6] found that some Facebook users gain gratification from the site by either social surfing, finding more information about other people, or expanding their social network. To find others and be found, users may fill out information on their profile and tailor their privacy settings to reach a wider audience. By doing so, these users are providing more information to the phishing attackers and exposing themselves as vulnerable targets. Lampe et al. [7] noted that there is a correlation between the completeness of profile details and the amount of online friends.

Additionally, users who are receptive to new connections may also be vulnerable to accepting friend requests and messages from attackers posing as legitimate users. Furthermore, users with large amount of friends may be more vulnerable to interacting with unknown strangers or unaware that their friends' accounts have been compromised. Vishwanath [15] performed a study in which he made friend requests and requests for private information using fake Facebook profiles. He found that habitual users of Facebook are more likely to both accept the fake friend requests and give up their private information than less frequent Facebook users. Patil [11] conducted a study of fake accounts in social networking sites (SNS) in 2012, in which they find that up to 40% of users would accept a fake account request. Boshmaf et al. [2] developed the Socialbot Network, a group of adaptive social bots that tricked up to 80% of Facebook users into accepting their friendship requests.

With all of these factors taken together, the high success rates reported for phishing through social media platforms may be considered unsurprising.

Other than our own prior work [12], however, we have not found any study on whether users treat links from these fake accounts the same as those from accounts connected to them based on relationships that extend beyond Facebook. Furthermore, no studies that we know of examine whether and how users are looking for indicators of compromised accounts or fake posts.

3 Methodology

We conducted the vignette study in a lab setting, as approved by the Institutional Review Board at Rochester Institute of Technology. The participants completed a survey hosted on the Qualtrics platform after they had read and agreed to informed consent document. In contrast to our previous work [12], this study used vignettes to investigate users' clicking behavior in different scenarios. Each vignette presented a unique combination of the variables that we explored: relationship between the post author and the participant, the location of the post, and the type of post.

Each vignette presents one combination of values for each variable. The values for the relationship between the post author and the participant are: Spouse/Partner, Close Friend, Acquaintance, and Public Page. There are four different values for post location: the participant's wall, the post author's wall with the participant tagged, the post author's wall without the participant tagged, and the participant's messenger inbox. The values for the types of post include: Interactives (e.g. quizzes), Sales-Oriented, and Media.

We had a total of 48 different vignettes considering all combinations of values for the variables. Instead of tiring out the participants with questions about all 48 vignettes, two of the four relationships were randomly selected for each participant. Therefore, each participant needed to respond to 24 individual vignettes. For each relationship, the participants were asked to provide a pseudonym to be used in the vignette to encourage familiarity, as well as some information about the person's Facebook usage behavior as observed by the participant in real life. For example, if a participant provided a pseudonym of "Tom" for her Spouse, a vignette was presented to the participant as following: "*Scenario 1: Tom has shared a post on your wall. It's an interactive post (e.g. quizzes, games).*" Then the participant was asked about how often she encounters this scenario in real life and how likely she is to click on that post.

We recruited 20 participants for this study—10 men with an average age of 23 and 10 women with an average age of 24. All of them were students at the Rochester Institute of Technology (undergraduates: 7, graduate students: 13). Each participant was compensated with a $10 Amazon.com gift card at the end of the session.

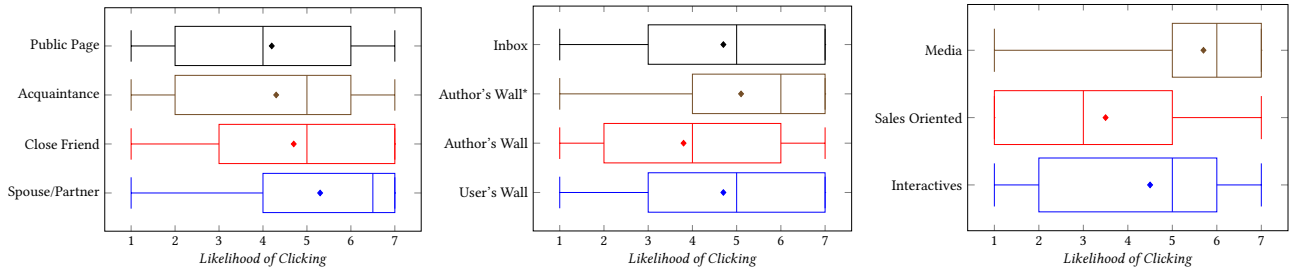
4 Findings

In this section, we report the results from our study. Due to a small sample size, we did not conduct any significance tests.

Our results show that the closer the relationship with the post-author, the higher the likelihood of clicking on a post. As shown in Figure 1a, posts shared by Spouse/Partner scored an average of 5.3 (on a 7-point Likert-scale), while the posts shared by Public Pages scored an average of 4.2. Furthermore, since all relationship types scored similarly on the frequency of their posting (between 'at least once a day' and 'at least once a week'), our results demonstrate that the closeness of relationship with post-author plays a role on users' clicking decisions.

In regards to the place of posting, our results show that when the post is shared in a location that is more noticeable to the user (e.g., the user's wall, the author's wall with the user tagged, and the user's inbox), the user is more likely to click. As shown in Figure 1b, posts shared on the author's wall (with tagging) scored an average of 5.1, posts shared on user's wall and in the messenger (i.e., inbox) scored an average of 4.7, while posts shared on author's wall (without tagging) scored the lowest: 3.8. This result differs slightly from our previous work, where we did not find any differences between the scenarios [12]. However, our new findings make more sense, since the locations that scored higher usually result in a notification that alerts the users to the post. Furthermore, when authors post on a user's wall, tag her in a post, or send her a private message, they are directly inviting her to interact with the post and start a conversation. Therefore, users are more inclined to click on such posts.

Figure 1c shows the effect of the type of the post. Sales-oriented posts scored the lowest with an average of 3.5 compared to interactive (4.5) and media posts (6.7). In previous work [12], we used



(a) Based on relationship **(b) Based on place (*Tagged)** **(c) Based on post type**

Figure 1: Likelihood of a user clicking a post based on three factors about the post (7-point Likert scale).

a different set of categories for the type of post (travel, news, and entertainment) which did not yield a noticeable difference in the likelihood score. In this regard, the new categories that we used in this study offer better distinctions.

In the survey, we asked participants to report how likely the person in each relationship is to share each type of post in real life. We then measured the likelihood of participants to click on a post that is similar to (or different from) the type of posts the author is more likely to share. We found a positive correlation between the likelihood of a post-author to share a particular type of post and the likelihood of the user to click on such a post shared by that author (see Figure 4). For example, if a participant reports that her spouse is more likely to share a media post, then she is more likely to click on a media post than the sale-oriented or interactive posts shared by her spouse. Similarly, participants are more likely to click on a post that they expect to be shared by a public page (e.g., sale-oriented page sharing a sales related post) than a relatively unexpected post, like a media page sharing a sales-related post.

We found a weak negative correlation between the likelihood of clicking on a post and the difference in post type from what is likely to be shared by a post-author (see Figure 4). This means, if the users encounter a post that they believe are not usually shared by the post-author, they are less likely to interact with them. However they are not strongly discouraged or deterred by this kind of mismatch.

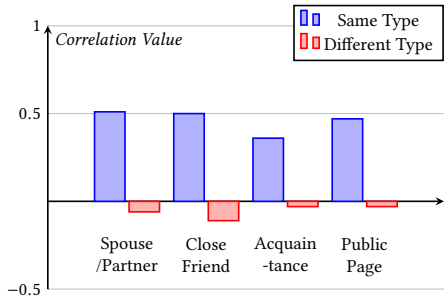


Figure 2: Correlation between the Likelihood of Sharing and Clicking on a Post Based on the Type of Post

5 Conclusions

In this vignette study, we have explored the relationship between whether users will click on a social media post and the attributes of the post, including who posts it, where it is posted, and the type of post. Attackers seeking to phish users on Facebook likely leverage this kind of information to craft their attacks, so it is important to understand for designing mechanisms to protect users.

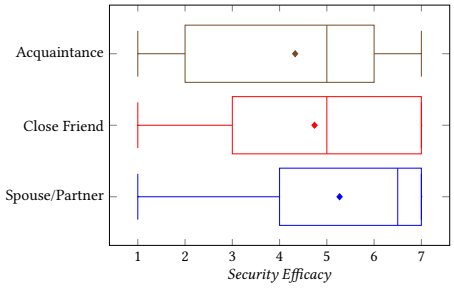


Figure 3: Correlation between the Likelihood of Sharing and Clicking on a Post Based on the Type of Post

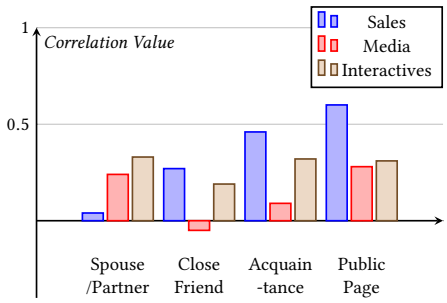


Figure 4: Correlation between the Likelihood of Sharing and Clicking on a Post Based on the Type of Post

References

[1] Safwan Alam and Khalil El-Khatib. 2016. Phishing Susceptibility Detection Through Social Media Analytics. In *Proceedings of the 9th International Conference on Security of Information and Networks (SIN '16)*. ACM, New York, NY, USA, 61–64. https://doi.org/10.1145/2947626.2947637

[2] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. 2011. The Socialbot Network: When Bots Socialize for Fame and Money. In *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC '11)*. ACM, New York, NY, USA, 93–102. https://doi.org/10.1145/2076732.2076746

[3] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the 24th SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, Montreal, Quebec, Canada, 581–590. https://doi.org/10.1145/1124772.1124861

[4] Susan Gonzalez. 2019. The Facebook phishing scam you should know about. https://www.thedenverchannel.com/news/national/the-facebook-phishing-scam-you-should-know-about

[5] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. 2007. Social phishing. *Communication of the ACM* 50, 10 (Oct. 2007), 94–100. https://doi.org/10.1145/1290958.1290968

[6] Adam N. Joinson. 2008. Looking at, Looking Up or Keeping Up with People?: Motives and Use of Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. ACM, New York, NY, USA, 1027–1036. https://doi.org/10.1145/1357054.1357213

[7] Cliff A.C. Lampe, Nicole Ellison, and Charles Steinfield. 2007. A Familiar Face(Book): Profile Elements As Signals in an Online Social Network. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. ACM, New York, NY, USA, 435–444. https://doi.org/10.1145/1240624.1240695

[8] Ben Litton. 2017. Study Finds Social Media Phishing Scams To Be The Most Dangerous. https://www.excaltech.com/study-finds-social-media-phishing-scams-dangerous/

[9] Phil Muncaster. 2017. Social Media Phishing Attacks Soar 500%. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

[10] Lindsey O'Donnell. 2019. Ultra-Sneaky Phishing Scam Swipes Facebook Credentials. https://threatpost.com/sneaky-phishing-scam-facebook/141869/

[11] Sameer Patil. 2012. Will You Be My Friend?: Responses to Friendship Requests from Strangers. In *Proceedings of the 2012 iConference (iConference '12)*. ACM, New York, NY, USA, 634–635. https://doi.org/10.1145/2132176.2132318

[12] Sovantharith Seng, Mahdi Nasrullah Al-Ameen, and Matthew Wright. 2018. Understanding users' decision of clicking on posts in Facebook with implications for phishing. In *Workshop on Technology and Consumer Protection (ConPro 18)*. https://www.ieee-security.org/TC/SPW2018/ConPro/papers/seng-conpro18.pdf

[13] Michail Tsikerdekis and Sherali Zeadally. 2014. Online deception in social media. *Communication of the ACM* 57, 9 (Sept. 2014), 72–80. https://doi.org/10.1145/2629612

[14] Verizon. 2019. Data Breach Investigations Report 2019. https://enterprise.verizon.com/resources/reports/dbir/

[15] Arun Vishwanath. 2014. Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication* 20, 1 (2014), 83–98. https://doi.org/10.1111/jcc4.12100