3-22-2019

Suspicion in Phishing and Organization Risk

Jonathan Coppola
University of Tampa, dhouse@ut.edu

Deanna House
University of Tampa, dhouse@ut.edu

SUSPICION IN PHISHING AND ORGANIZATION RISK

Jonathan Coppola
University of Tampa
jonathan.coppola@spartans.ut.edu

Deanna House
University of Tampa
dhouse@ut.edu

ABSTRACT

Phishing emails are communications that are sent out in mass and are designed with the goal of obtaining sensitive information, installing malware on a user's machine, or gaining access to a network. Training users about the dangers of phishing emails is common in organizations, but users will still frequently fall victim to phishing attacks. Organizations may feel that they are doing the necessary actions, such as providing user security training, to mitigate the risk of users' lack of secure behavior. Organizations are faced with the challenge of the human element; the most undependable and uncontrollable part of an information system. As time has progressed, corporations are beginning to understand that they must put measures and controls into their security IT to mitigate the possible problems that arise from human interaction with IT. This research attempts to explore suspicion as it relates to emails and how-to better train individuals to recognize illegitimate emails.

Keywords

Suspicion, phishing, behavioral security, security training

INTRODUCTION

Phishing emails are communications that are sent out in mass and are designed so that users can easily click on a provided link and give out requested sensitive information. The emails have a goal of gaining access to information such as logins/passwords or other information that can be used to gain access to a person's identity, installing malware on a user's machine, or gaining access to a network. Frequently, the emails are so good that the recipient and/or organization does not even know that the email was fraudulent and clicked on until a scan indicates malware is detected or a data breach occurs. Even more problematic are the more-targeted spear phishing attacks. These campaigns frequently have more personalized information for email recipients making the detection more difficult and potentially more dangerous.

According to Posey (2015), phishing emails can be spotted by the following:

Mismatched URL
URL with misleading domain name
Poor spelling/grammar
Asks for personal info
Too good to be true
Action not initiated
Asked for money
Unrealistic threats
From a government agency
Something doesn't look right

Table 1: Spotting a Phishing Email (from Posey, 2015)

Table 1 above lists ways to spot a phishing email. While some items in the list are fairly easy for an individual to understand and implement (such as mismatched URL, poor spelling/grammar, or asks for money), the item "something doesn't look right" is more difficult for an individual to pinpoint. The suspicion that can be triggered by something in an email that seems off can be challenging.

Phishing emails can be a serious problem for organizations due to the risk of malware getting into an its network. In a study by Benenson et al. (2017), it was found that 56% of people will click on links in emails. A lower percentage will tell someone that they clicked a link than the actual amount of people who do. This means that not only are the security professionals faced with keeping up with all the new types of malware and cyber threats, but they need to continuously be watching the network for uncommon forms of traffic. This creates a strain on the professionals because they are facing a multiple front battle that people from within their own organizations are not helping with. This exploratory research will identify keywords that can be included in emails that trigger suspicion and can be used to subsequently develop training.

LITERATURE

According to Meriam-Webster dictionary, suspicion is defined as "a state of mental uneasiness and uncertainty" (Suspicion, 2018). This differs from what the empirical definition that most researchers believe in. The reason for this is the fact that the research community cannot come up with a consensus as to what the definition is. According to Bobko, after conducting a literature review, the construct of suspicion has never really been defined and most researchers are using the psychological definition of the state of suspicion, but never really define it. (Bobko, 2014). There are several areas that can be built upon related to what happens when an individual receives an email that requires a decision.

External Factors Related to Decision Making

One such factor is key words or phrases. The power of communication and words can sometimes be extremely underappreciated and undervalued. Certain words or key phrases can cause people to feel a certain way about a situation. They could also trigger memories which can influence a person's decisions. In addition environment is an influence in decision-making. Both the current environment and the environment that an individual was raised in will influence different factors. Individuals have had different experiences in their environment and thus are choosing based on those.

Evaluating the current environment such as the corporate culture of a company can cause one to want to do what may be necessary to keep and/or perform their job. This relates to Maslow's level of love and belonging. The environment that one finds themselves in at any given moment may be a factor in their decision-making process.

Suspicion as an Emotion

According to Leighton, "Emotions stem from judgements of a situation." This falls into theme with the previous statements about how one's upbringing changes one's perception of a situation. This causes the dilemma spoken of above where researchers are not able to truly define an empirical definition for what suspicion is. What makes one person happy may make one person sad. The same falls true for suspicion in people. Because there is no one instance where every single person becomes suspicious, it is hard to declare certain situations where one can state with certainty that a majority of the people involved would become suspicious within a statistically valid percentage. The use of keywords as suspicion markers will assist in the identification of methods that can be widely applied.

Phishing Scam and Suspicion

The definition of a phishing scam is "a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information". (Phishing Attacks, 2018). One problem that many people are noticing is that even though people know that there is a risk for a phishing

attack they still click on the link. According to research conducted by Benenson et al., 2014, the percentage of people doing this could be as high as 56%.

This is a serious problem for cyber security professionals because it is one of the leading causes of malware being able to make its way onto an organizations network. Further study findings by Benenson et al. (2014) indicated that while 56% of participants clicked on links in email; people were less likely to a lower percentage of people told someone that they clicked a link. This means that not only are the security professionals facing keeping up with all the new types of malware and cyber threats, but they need to continuously be watching the network for uncommon forms of traffic. This creates a strain on security professionals because they are facing a multiple front battle that people from within the organization are not helping with.

Another problem stemming from this issue is that phishing is the most correlated type of attack to ransomware. Ransomware is defined as "a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key." (Ransomware, 2018) As one can imagine this is a big problem for organizations, because if its cyber team cannot get the files decrypted, or does not have a backup of said files, then the only way to get said files back would be to pay the adversary for the decryption. This puts a strain on recovery plans to the organization because you cannot truly prepare for the amount the hacker will be requesting. Organizations need to keep this on the radar because according to PhishMe the rate of phishing emails increased from 92% in quarter 1 of 2016 to 97.25% during quarter 3. (Ransomware Delivered by 97% of Phishing Emails by end of Q3 2016 Supporting Booming Cybercrime Industry, 2016)

Continuing on with problems that organizations are facing, according to Crowe, "52% of organizations that faced a cyber security incident in 2016 are not planning on making any changes in 2017." (Crowe, 2016) This makes the job of cyber security professionals even more difficult because it showcases that many businesses are only focused on their bottom line and see technology as a way to get there. This is a problem because even though information exchange and technology is becoming the overlying basis of productive and successful organizations, the security of said organizations and information needs to be addressed.

Emotional Awareness

Emotional awareness would encompass training employees to be self-aware of emotions on a greater scale while in the work place. As mentioned above, the proposed research would look into how different key words in phishing scams would elicit different emotions from people would allow for professionals to take those results and possibly develop tailored training plans based on how people react to different scams.

Placing training like this into overall training plans would allow for the overall develop of employees to see when emails might possibly be purposefully geared towards enticing them to click on the phishing link. If this can possibly be achieved, the overall success rates of phishing scams would decrease and therefore eventually become obsolete in terms of getting peoples information.

Technical Awareness

As discussed before one of the problems cyber professionals are facing today is the fact that many of upper management and board members are not "buying" into the understanding that advancements in technology will always come with a price. Unfortunately, not all new technological advancements are designed with security in mind. With that understanding, early adopters, or those that designed to incorporate a technology in its early stages, know that there is an automatic risk associated with a new technology.

Along these lines, a majority of people either know that there is risk involved and do not care, or don't understand that technology itself comes with an inherit risk to begin with. By training people to understand how technology can be used against them or the company as a whole and the possible implications, the likelihood of people to just jump into technology would decrease. In addition, the likelihood of people to understand why the technology team puts the limitations and policies in place for the overall security of the company. Being able to change people's perception to one of that instead of one of the IT just being difficult would help the overall job of the IT team instead of it being a two front battle.

Social Awareness

The final type of awareness to be discussed is social awareness. This would be defined as understanding how technology plays an impact on our society itself and how it can be used against us in the same sense. An example of that is with phishing itself. One thing that is the unfortunate thing with the spread of information sharing is that it has become a common practice in many organizations to share links through emails. Along with this has grown peoples wanting to note only share business information but also websites, videos, and personal links with others. This has desensitized many to the fact of links potentially leading to harmful or malicious sites.

The overall problem is that too few people really care about this problem for what it is and will instead follow others maladaptive behavior. This is hard to break because it is within our social nature to want to be with the crowd. However, if researchers are able to come up with a way to dissuade people from their nature and be aware that our innate nature is causing security issues, we will be able to begin to shift focus from being within the pact to making sure the company is secure.

PROPOSED RESEARCH

The next steps of this research will entail exploring the types of email keywords that arouse suspicion. The researchers will use the Thesaurus-Snowball technique (Jehn & Werner, 1993) to come up with keywords/synonyms related to the term suspicion. These words are: doubt, misgiving, thought, distrust, feeling, mistrust, notion, disbelief, wariness, inkling, question, skepticism, apprehension, idea, and hunch. Each of these synonyms are also explored, which results in a snowball effect and a list of terms related to the word suspicion. During the second phase of the research, the researchers will evaluate actual phishing emails and pair with existing research to determine a list of words/terms that will invoke suspicion. The researchers will use text analysis to determine words and terms that arouse suspicion that are frequently present in phishing emails. This method is similar to that used by Doucet & Jehn (1997). Then similarly designed phishing emails would be made with different key words changed to try and elicit different emotions from participants to explore the click rate on links and collect additional data related to the motivations for clicking. The researchers will design email messages that are categorized with levels of suspicion levels (low, moderate, high). Low suspicion messages will have 1 marker, moderate suspicion messages will have 3 suspicion markers, and high suspicion messages will have 5 suspicion markers. The research will also attempt to determine truth accuracy for phishing message detection. Users are not accurate at detecting phishing websites, even when primed (Alsharnouby et al, 2015). In addition, after the experimental data is collected, survey data will be collected explore perceived trust, source credibility, state level suspicion, phishing familiarity and the effects that these variables have on the accuracy of message detection (legitimate and illegitimate).

doubt	disbelief
misgiving	wariness
thought	inkling
distrust	question
feeling	skepticism
mistrust	apprehension
notion	idea
hunch	

Table 2: Level 1 Suspicion Terms, Microsoft Word Thesaurus, 2016

This proposed research would help determine which keywords arouse the greatest level of suspicion while also exploring the accuracy of message detection. Phishing message suspicion has not been explored previously in this manner. Overall the project will be beneficial to the cyber community as a whole in creating a new viewpoint in combating a major threat.

CONCLUSION

The focus of this paper was to explain what causes people to click on phishing emails and why this should be an interest to the cybersecurity community. We explored the idea that suspicion is an emotion, and that people can be trained to understand their emotions. By looking into which, if any, keywords entice people to click on phishing emails more than others and which keywords arouse suspicion we can create and improve upon training programs specific to making people aware of said keywords and therefore decrease the amount of successful phishing attacks by determining the affects that suspicion has on phishing message detection accuracy.

We also explored how generating better training programs for social, technological, and emotional awareness would allow for an overall better understating about how even though technology is useful in the business place it also allows for more vectors of risk and therefore needs to be better understood and appreciated. Hopefully, the goal of this paper has been seen and exploration into the causes of successful phishing attacks from a social aspect will be better researched.

REFERENCES

1. Alsharnouby, M., Alaca, F., & Chiasson, S. (2015) Why Phishing Still Works: User Strategies for Combating Phishing Attacks. *International Journal of Human-Computer Studies*, 82, C, 69-82.
2. Benenson, Z., Girard, A., Hintz, N., & Luder, A. (2014) Susceptibility to URL-Based Internet Attacks: Facebook vs. Email. *IEEE International Conference on Pervasive Computing and Communication Workshops*, March 24-28, 2014, Budapest, Hungary.
3. Benenson, Z., Gassmann, F., & Landwirth, R. (2017) Unpacking Spear Phishing Susceptibility. *Targeted Attacks*, 1-17.
4. Bobko, P., Barelka, A.J., Hirschfield, L.M., Lyons, J.B. (2014) The Construct of Suspicion and How It Can Benefit Theories and Models in Organizational Science. *Journal of Business and Psychology*, 29, 3, 335-342.
5. Crowe, J. (2016) *Cyber Attack Statistics: Majority of Victims Aren't Changing Their Security in 2017*. Retrieved from Barkly: https://blog.barkly.com/cyber-attack-statistics-2016.
6. Doucet, L. & Jehn, K.A. (1997) Analyzing Harsh Words in a Sensitive Setting: American Expatriates in Communist China. *Journal of Organizational Behavior,* 18, 559 – 582.
7. Jehn, K. & Werner, O. (1993) Theory, A Thesaurus, and Word Frequency. *Cultural Anthropology Method*, 5, 8-10.
8. *Phishing Attacks*. (2018) Retrieved from Imperva Incapsula: https://www.incapsula.com/web-application-security/phishing-attack-scam.html
9. Posey, B. (2015) 10 Tips for Spotting A Phishing Email. Retrieved on December 20, 2018 from http://www.techrepublic.com/blog/10-things/10-tips-for-spotting-a-phishing-email/
10. *Ransomware*. (2018) Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/definition/ransomware
11. *Ransomware Delivered by 97% of Phishing Emails by end of Q3 2016 Supporting Booming Cybercrime Industry*. (2016) Retrieved from Cofense: https://cofense.com/ransomware-delivered-97-phishing-emails-end-q3-2016-supporting-booming-cybercrime-industry/
12. *Suspicion*. (2018) Retrieved from Meriam-Webstrer: https://www.merriam-webster.com/dictionary/suspicion?utm_campaign=sd&utm_medium=serp&utm_source=jsonld
13. Vishwanath, A., Harrison, B., & Ng, Y.J. (2018) Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research,* 45, 8, 1146 – 1166.