Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2018 Proceedings

Midwest (MWAIS)

5-2018

Got Phished! Role of Top Management Support in Creating Phishing Safe Organizations

Gaurav Bansal
University of Wisconsin – Green Bay, bansalg@uwgb.edu

Got Phished! Role of Top Management Support in Creating Phishing Safe Organizations

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

ABSTRACT

In this research, we examine the role of top management involvement in creating phishing awareness in an organization. This study deploys field study experiment with phishing deception. The study was carried out in two phases – phase 1 involved training the employee-participants of a Midwestern US University randomly using two different phishing awareness training videos – one showcasing chancellor of a Midwestern University, and another one showcasing a newly hired IT officer. Phase 2 involved three phishing attacks with varying regarding the degree of sophistication (or social engineering). The results show that there is a significant positive impact of perceived top management involvement in creating phishing awareness and preventing employees from getting phished. The paper concludes by discussing theoretical and managerial implications.

Keywords

Top management involvement, social engineering, phishing attack, field study

INTRODUCTION

Cybercriminals utilize phishing to launch cyber attacks on organizations. A clear majority of organizations (76%) reported experienced phishing attacks in 2017 (Seals 2018). There are several reasons why employees get duped by phishing emails – such as curiosity, fear, urgency, reward/recognition, and opportunity (Zurier 2016). Phishing relies on social engineering techniques to persuade users to divulge private and sensitive information (Harrison et al. 2016). Social engineering is defined as the "'art' of influencing people to divulge sensitive information" (Mouton et al. 2016 p. 187).

Information security is an organization-wide issue, and it is no surprise that it takes an entire organization and top leadership to create security awareness and to prevent employees from getting "phished." Prior research suggests that top management commitment impacts degree of security awareness in the organization (Hansche 2001; Power 2007; Tsohou et al. 2015). Top management and organizational culture are also known to enhance employee compliance with information security policies (Hu et al. 2012; Knapp et al. 2006), however, till date, there is little research examining the role of top management support in creating phishing aware and cyber-safe organizations. While Knapp et al. (2006) find a positive correlation between top management support and security culture as well as security policy enforcement, further investigation is needed to establish the causal relationship between top management involvement and the effectiveness of organizational security strategies and programs (Beznosov and Beznosova 2007). There is limited research delving into how top management involvement can help create awareness for employees to detect and safeguard themselves against regular phishing and highly-targeted spear-phishing[1], whaling or business email compromise[2] attempts. This study attempts to fill that gap.

Phishing messages are of several different types such as regular phishing, spear-phishing, whaling, business email compromise (BEC/CEO email fraud), and clone phishing - depending upon the profile of the victim, and nature of the message (pl see CSOonline.com 2017 for definitions of these terms). Spear-phishing, whaling and BEC phishing messages deploy a high degree of sophistication and social engineering and hence have higher "success" rate (Wang et al. 2016). Cyber attackers are increasingly utilizing such tools to launch data breaches. According to symantec.com (2017), more than 400 businesses are targeted by BEC messages every day. Such advanced phishing messages use psychological factors such as fear (of losing something), anticipation (of gaining something), urgency, and perceived legitimacy to deter the users from focusing on the underlying detectors (Goel et al. 2017).

[1] https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109
[2] https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

The study examines the following two research question: (a) role of social engineering on likelihood of getting phished, and (b) role of top management involvement in creating phishing awareness. The next sections explain the constructs, define hypotheses, and elucidate the methodology and analysis. After a discussion of the findings, implications for research and practice follow.

THEORY & RESEARCH MODEL

Sophisticated phishing attacks (such as whaling, business email compromise among others) involve a high degree of social engineering tactics to distract the user from the underlying deception indicators. The degree of sophistication and distraction (such as urgency, the title of the sender) impairs the effect of any phishing awareness training (Caputo et al. 2014; Wang et al. 2013). Increasing number of phishing emails are using social engineering tactics (verizonenterprise.com 2013). A report by TrendMicro.de (2012) suggests that 91 percent of all targeted attacks involve spear-phishing. Spear phishing attacks have a high success rate, and therefore remain one of the leading causes of data breaches (Verizonenterprise.com 2017) and are increasingly being used to target business of all sizes (smallbiztrends.com 2016; Verizonenterprise.com 2017).

Using deception theory, Wang et al. (2012) found that emotional triggers (such as urgency, attention to title) play a much stronger decisive role than the phishing detection indicators (such as spelling/grammar mistakes, spoofed email address) on the likelihood of responding to a spear-phishing message. Wang et al. (2012) explain that such emotional or "visceral triggers" (p. 345) limit one's use of the cognitive energy available for processing and detecting the phishing email message. Hence,

H1: There is a positive association between the degree of social engineering of a phishing email message and the user's likelihood of getting phished.

Top management participation is known to strongly influence organizational culture as well as employees' attitudes towards compliance with information security policies (Hu et al. 2012)). According to Hu et al. (2012), top management exerts the organizational influence via three mechanisms: legitimacy, commitment and perceived fairness and procedural justice. By participating in security initiatives the top management provides legitimacy to the security programs, convey a sense of commitment to security policies, and provide opportunities for employees to exercise control, thus, contributing to the perceived fairness and procedural justice (Hu et al. 2012). We argue that top management involvement will positively impact employee's attitude and behavioral control towards phishing awareness. However, based on training limitations with spear phishing (Wang et al. 2012) we contend that such top management involvement will have a more profound effect on low-to-medium sophistication phishing messages than on high sophistication phishing messages (spear phishing). Hence,

H2: There is a negative association between top management involvement and the likelihood of getting phished, and this relationship is stronger for low/medium (as opposed to high) socially engineered phishing messages.

RESEARCH METHODOLOGY

The research was conducted using a field experiment approach. We gathered data from faculty and staff of a Midwestern US university. Request to participate in the research survey was emailed to the entire University employees from provost office. 853 faculty and staff of a Midwestern University were invited to participate in the study. They were incentivized to participate in the study by having their email id entered in for $50 gift card drawings. We conducted the study in two phases. In phase 1 participants were shown a phishing awareness training video which was inspired by the message from https://www.stopthinkconnect.org (see Appendix A). Respondents were randomly assigned to watch a phishing training video offered showcasing the University Chancellor himself, or the one showcasing a newly hired IT officer, and were asked permission to participate in phase 2 (computer intervention) by providing their email address. In phase 2 – we carried out phishing attack using three different types of email messages differing in degree of social engineering involved (LSS: low sophistication, MSS: medium sophistication, and HSS: high sophistication). Top management was operationalized by showing Chancellor's video, as compared to IT officer's video. Both the videos had exact same content.

Experiment

In total 168 employees participated in phase 1 of the study. The average age was 44.37 (n=129), ranging from 24 to 72, and the standard deviation was 11.99 years. There were 37 males and 96 female respondents. 117 employees provided a valid university email address. In phase 2 – 117 employees who provided their valid email address (in phase 1) were contacted with three different phishing email messages spread over a week's time. The phishing messages differed regarding the degree of social engineering used. LSS phishing message required people to click on a link to download the Microsoft updates and appeared to be coming from Microsoft. MSS phishing message appeared to be coming from the University's IT department and required people to click on a link to complete their IT training. HSS phishing message appeared to be coming from the University's chancellor's office and asked respondents to click on a link to provide feedback on recent developments that have happened in the University. The messages are available in Appendix B. Six employee-participants got phished in LSS. Twenty-eight employee-participants got phished in the MSS with 15 employee-participants clicking on the link more than once, ranging from 2 clicks to 12 clicks, with the mode being four clicks each for five employee-participants. Forty-eight employee-participants got phished in HSS with 20 employee-participants clicking on the link more than once, ranging from 2 clicks to 8 clicks, with the mode being two clicks each for nine employee-participants. 19 employee-participants clicked on both MSS and HSS links; 4 employee-participants clicked on the links in both LSS and MSS, and four employee-participants clicked on the links in both LSS and HSS messages.

Experiment timeline:

Phase1: We sent out two invitations 19 days apart - 116 employees responded to the first call (wave 1), and 52 employees responded to the second call (wave 2). Between the two waves, there was no significant difference regarding age, and number of clicks in LSS, MSS or HSS messages. In phase 2 of the research, we carried out a computer-based intervention (phishing attack). Three phishing attack occurred between day 25 and day 32 (counting from the day when the first call was sent out). Three phishing email messages (LSS, MSS, and HSS) were sent out to every respondent (n=117) who provided with a valid email address to participate in phase 2. The three types of messages were sent in a random order to avoid any order effect. Table 1 provides an overview of the number of clicks in phase 2 arranged per the type of the video shown in phase 1.

Data Analysis and Results

Data analysis was carried out using SPSS (IBM Corp. 2016). We analyzed the data using Pearson Chi-square (for both H1 and H2). We found support for both the hypotheses. H1: Results show that more employee-participants got "phished" with HSS than with MSS (χ^2 = 10.953, df=1, p=.001), and also more with MSS than LSS messages (χ^2 =6.345, df=1, p=.012). H2: Results (Table 2) reveal that significantly fewer number of employee-participants who saw Top Management i.e. chancellor's video (as opposed to IT officer's video) got phished by MSS messages. However, in case of HSS (and also LSS), there was no significant difference of the type of video watched (chancellor's vs. IT officer's) on the number of employee-participants who got phished. Note: We could not identify the video shown (chancellor's or IT officer's for these respondents), however we did record how they responded to the type of phishing email message (LSS, MSS or HSS). Hence we used these respondents in computing H1, but not for H2.

		Phase 2								
		LSS			**MSS**			**HSS**		
		0 Clicks	**1 Click**	**>1 Clicks**	**0 Clicks**	**1 Click**	**>1 Clicks**	**0 Clicks**	**1 Click**	**> 1 Clicks**
Phase 1	Video Shown not recorded	23	1	1	21	1	3	13	6	6
	Chancellor's Training Video (Top Mgmt)	47	0	1	41	3	4	33	10	5
	IT Officer's Training Video	41	1	2	27	9	8	23	12	9

Table 1. Training Video and Phished Crosstab Analysis

<>

Phishing scenario	Pearson Chi-Square	P value
LSS	1.597/df=2	.450
MSS	8.394/df=2	.015
HSS	3.215 / df=2	.200

Table 2. Chi-square Test Results

DISCUSSION

The research shows that there is a difference between the degree of social engineering involved and the likelihood of getting phished and it also shows the critical role of top management involvement (via training videos) in creating phishing awareness among employees - thus creating more secured organizations. The findings suggest that employee-participants were aware of "generic" phishing emails -- as only 6 out of 120 employees clicked on LSS messages; and they responded with caution for MSS messages when trained by Chancellor's phishing awareness video as compared to newly hired IT officer's video. The findings for HSS are consistent with prior research by Caputo et al. (2014) which found that training has limited effect in preventing spear phishing attacks.

Spear phishing is a very sophisticated way of targeting employees and training is known to have little effect in preventing such highly socially-engineered attacks (Caputo et al. 2014). User's lack of knowledge of phishing attacks (Lötter and Futcher 2015), attention to emotional cues (Wang et al. 2012), and fear of losing or anticipation of gain (Goel et al. 2017) cause the users to fall victim to such attacks. This study shows that training and top management involvement can only do so much in creating safe organizations when it comes to BEC/CEO email fraud. Future research could look into other individual factors such as mindfulness (Jensen et al. 2017) in creating safe organizations. Future research can also look into the role of cultural traits such as power distance (Bullee et al. 2017), masculinity/femininity, and uncertainty avoidance in responding to spear-phishing messages.

The paper makes several contributions. First, it shows the role of degree of social engineering on the likelihood of getting phished. Second, it adds to our understanding of the relationship between top management involvement and the likelihood of getting phished. Third, mainstream MIS literature has looked at phishing problems primarily from two perspectives: technical – e.g., (Abbasi et al. 2015; Zhang et al. 2014); and behavioral – e.g., (Jensen et al. 2017; Moody et al. 2017; Wright and Marett 2010). This paper adds another dimension to the phishing research in MIS stream – the role of top management involvement – and thus has substantial theoretical implications as well.

ACKNOWLEDGMENT

Author is grateful to Travis Albrecht for help in designing the phishing emails; Janet Bonkowski and Mike Schmitt for video recordings; Steve Muzatko and Wenkai Zhou for help with survey testing; and last but not the least, Chancellor of the host University for his overall support. The research was made possible in part due to Frederick E. Baer Professorship in Business.

REFERENCES

Abbasi, A., Zahedi, F. M., Zeng, D., Chen, Y., Chen, H., and Nunamaker, J. F. 2015. "Enhancing Predictive Analytics for Anti-Phishing by Exploiting Website Genre Information," *Journal of Management Information Systems* (31:4), p. 109.

Beznosov, K., and Beznosova, O. 2007. "On the Imbalance of the Security Problem Space and Its Expected Consequences," *Information Management & Computer Security* (15:5), pp. 420-431.

Bullee, J.-W., Montoya, L., Junger, M., and Hartel, P. 2017. "Spear Phishing in Organisations Explained," *Information & Computer Security* (25:5), pp. 593-613.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., and Johnson, M. E. 2014. "Going Spear Phishing: Exploring Embedded Training and Awareness," *IEEE Security & Privacy* (12:1), pp. 28-38.

CSOonline.com. 2017. "Types of Phishing Attacks and How to Identify Them." from https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html

Goel, S., Williams, K., and Dincelli, E. 2017. "Got Phished? Internet Security and Human Vulnerability," *Journal of the Association for Information Systems* (18:1), pp. 22-44.

Hansche, S. 2001. "Designing a Security Awareness Program: Part I," *Information Systems Security* (9:6), pp. 14-23.

Harrison, B., Svetieva, E., and Vishwanath, A. 2016. "Individual Processing of Phishing Emails: How Attention and Elaboration Protect against Phishing," *Online Information Review* (40:2), pp. 265-281.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp. 615-660.

IBM Corp. 2016. "IBM SPSS Statistics for Windows, Version 24.0. Armonk, NY."

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., and Nelson Ford, F. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security* (14:1), pp. 24-36.

Lötter, A., and Futcher, L. 2015. "A Framework to Assist Email Users in the Identification of Phishing Attacks," *Information and Computer Security* (23:4), pp. 370-381.

Moody, G. D., Galletta, D. F., and Brian Kimball, D. 2017. "Which Phish Get Caught? An Exploratory Study of Individuals′ Susceptibility to Phishing," *European Journal of Information Systems* (26:6), pp. 564-584.

Mouton, F., Leenen, L., and Venter, H. S. 2016. "Social Engineering Attack Examples, Templates and Scenarios," *Computers & Security* (59), pp. 186-209.

Power, M. 2007. "Developing a Culture of Privacy: A Case Study," *IEEE. Security and Privacy Magazine* (5:6), pp. 58-60.

Seals, T. 2018. "Three-Quarters of Businesses Saw Attacks in 2017 (Jan 17)." from http://informationsecurity.report/news-article.aspx?ID=4785

smallbiztrends.com. 2016. "43 Percent of Cyber Attacks Target Small Business (Jun 21)." from https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html

symantec.com. 2017. "2017 Internet Security Threat Report." from https://www.symantec.com/security-center/threat-report

TrendMicro.de. 2012. "Spear-Phishing Email: Most Favored APT Attack Bait." from https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2015. "Managing the Introduction of Information Security Awareness Programmes in Organisations," *European Journal of Information Systems* (24:1), pp. 38-58.

verizonenterprise.com. 2013. "2013 Data Breach Investigations Report." from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Verizonenterprise.com. 2017. "2017 Data Breach Investigations Report." from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Wang, J., Herath, T., Chen, R., Vishwanath, A., and Rao, H. R. 2012. "Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email," *IEEE transactions on professional communication* (55:4), pp. 345-362.

Wang, J., Li, Y., and Rao, H. R. 2016. "Overconfidence in Phishing Email Detection," *Journal of the Association for Information Systems* (17:11), p. 759.

Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. "The Association between the Disclosure and the Realization of Information Security Risk Factors," *Information Systems Research* (24:2), pp. 201-218,494-495.

Wright, R. T., and Marett, K. 2010. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *Journal of Management Information Systems* (27:1), p. 273.

Zhang, D., Yan, Z., Jiang, H., and Kim, T. 2014. "A Domain-Feature Enhanced Classification Model for the Detection of Chinese Phishing E-Business Websites," *Information & Management* (51:7), p. 845.

Zurier, Z. 2016. "91% of Cyberattacks Start with a Phishing Email (Dec 13)." from https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

APPENDIX A: TRAINING VIDEO SCRIPT

Cyber Security is our shared responsibility. It is up to each of us to make sure that we keep [university name omitted] information resources safe and secure.

Cybercriminals and Phishers want to steal your personal information and cause you harm. Links in emails are how they try to steal your information. They send emails that look legitimate but get you to do things that steal your information. They are counting on you to respond quickly without thinking about what you are doing. If you respond to these emails, it could cost our University and you. I recommend a three-prong strategy that you can exercise to prevent yourself from getting “phished”:

STOP! Think Before you Act! Connect!

STOP!
Stop to see if the email is from someone you recognize and trust, or are expecting. Do not immediately act on an email by downloading a file, clicking a link, or replying. Make sure that the name and *email address* match and seem legitimate.

Think before you act!
Consider for a moment what the email is asking you to do. Does the request ask for private or proprietary information? Is the request unexpected or rushed? Does the request make sense? Why would the sender need you to do this? Be wary of emails that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.

Connect!
I recommend that if something looks suspicious, delete it, or check with the IT helpdesk.
Also, please make sure that your passwords are unique and complex for each website and account. Remember never share your password with anyone, especially via email or through an email link.
Stay Cyber Aware and Go[redacted]!

APPENDIX B: PHISHING EMAILS USED IN THE STUDY

A. Low Sophistication Scenario (LSS) message

Fm: Help Desk
Subject: System Upgrade

Dear User,
Due to our new system upgrade. In order for it to remain active follow the link Sign in Re-activate your account to outlook. https://account.live.com.

Thanks,
The Microsoft Account Team.
Link above takes to page: Microsoft sign in landing page

B. Medium Sophistication Scenario (MSS) message

From: IT Dept <helpdesk@securityeducation.info>
Sent: Thursday, February 1, 2018 11:40 AM
To: [redacted]
Subject: Manditory Training
To all [redacted] employees,

Our campus IT policy requires all the employees to be trained in [redacted] **IT security policy**.
This link will take you to the [redacted] IT security policy site. This training is required every year. This yearly online training is intended to help you understand the [redacted] security policy requirements relating to best practices about keeping our information and IT resources safe on campus. The training should take about 15 minutes to complete. Please complete the training at your earliest convenience.
IT Dept.
[redacted]
Link shown above takes to a typical university's login landing page

C. High Sophistication Scenario (HSS) message

From: [redacted] [mailto:geoff@online-invite.com]
Sent: Friday, February 02, 2018 12:17 PM
To: [redacted]
Subject: Your feedback is required
University Community—
I would personally like you to take some to reflect upon the recent developments and share your thoughts with me. Please click on the following link to send your thoughts directly to me.

Signature / Chancellor