WISP 2019 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

12-15-2019

An expert assessment of corporate professional users to measure business email compromise detection skills and develop a knowledge and awareness training program

Shahar Aviv

Yair Levy

Ling Wang

Nitza Geri

An expert assessment of corporate professional users to measure business email compromise detection skills and develop a knowledge and awareness training program

Shahar Aviv[1]
College of Engineering and Computing, Nova Southeastern University
Fort Lauderdale, FL USA

Yair Levy
College of Engineering and Computing, Nova Southeastern University
Fort Lauderdale, FL USA

Ling Wang
College of Engineering and Computing, Nova Southeastern University
Fort Lauderdale, FL USA

Nitza Geri
Department of Management and Economics, The Open University of Israel
Ra'anana, Israel

ABSTRACT

Cybercrime against organizations is a daily threat and targeting companies of all sizes. Cyberattacks are continually evolving and becoming more complex. Cybercriminals utilize email attacks as their most used method to compromise corporations for financial gain. Email attacks have evolved into sophisticated scams which target businesses that conduct wire transfers as part of their business operations. The FBI has announced a new evolution of email attacks called Business Email Compromise (BEC) scams which utilize social engineering, phishing, and email hacking to manipulate employees into conducting fraudulent wire transfers. The goal of this study was to use cybersecurity experts to validate the BEC detection measurement criteria for user skills and an awareness training program amongst corporate professionals. BEC attacks have attributed to over $26 billion in financial losses across the globe and are continually increasing. A Delphi methodology was utilized to attain feedback from 30 cybersecurity experts to develop and validate the BEC detection measure and awareness training. Results show that

[1] Corresponding author. aviv@mynsu.nova.edu +1 954 254 8040

there are four contributing attributes to BEC detection: email authenticity detection skills, malicious mobile application detection skills, ability to detect mobile malware indicators, and the ability to detect phishing emails. The research study concludes with discussions and future research recommendations.

Keywords: Cybersecurity skills; phishing; business email compromise (BEC), mobile malware.

INTRODUCTION

The evolution of technology and increase in the utilization of public Internet based services such as cloud computing, social networks, as well as online money transaction services have greatly increased cyberattack risks for organizations (Bendovschi 2015). Corporations are becoming increasingly more connected to the open Internet, which in turn has increased the number of cyberattacks that have already affected seven million businesses including high profile attacks on corporations such as Target and JPMorgan Chase (Nandi Medal and Vadlamani 2016). Cyberattacks on businesses are increasingly becoming more complex and require a focus not only on the technical security aspects, but the organizational policies and human aspects as well (Roumani Fung and Choejey 2015). As emails have become a standard method of communication via the connected world, cybercriminals utilize email systems to conduct cyberattacks on businesses for financial gains (Deshmukh Shelar and Kulkarni 2014). The FBI has announced a new email-based scam on businesses called Business Email Compromise (BEC) attacks as it began to receive business complaints surrounding fraudulent wire transfer requests (FBI 2015). Traditional security methods, such as spam filters, have not been successful in blocking BEC attacks as they are custom and seem legitimate and have not been detectable via technical security solutions (Jakobsson and Leddy 2016). BEC attacks are sophisticated email scams that target businesses that conduct wire transfers as part of their standard operations (FBI Internet Crime Complaint Center 2015). These BEC attacks leverage legitimate business email accounts through hacking and social engineering methods to scam the victims into conducting wire transactions (FBI Internet Crime Complaint Center 2015). Social engineering is a key component within BEC attacks, where cybercriminals have been very successful in defrauding businesses and employees worldwide (Mansfield-Devine 2016). Furthermore, BEC attack methods also utilized in CEO fraud include gaining access to the corporate network through spear-phishing and malware attacks (FBI 2017). The most common types of phishing involve manipulating corporations and users for financial gain and include additional attack vectors such as social engineering, text, and voice conversations to increase the attack success rate (Furnell Millet and Papadaki 2019).

BEC attacks are increasingly becoming more difficult to detect with automated detection tools, therefore, there is a need for users' ability to detect and react to malicious email attacks (Stembert Padmos Bargh Choenni and Jansen 2015). BEC attacks are now attributed to over 166,000 BEC incidents globally with over $26 billion in reported financial losses to organizations of all sizes (FBI Internet Crime Complaint Center 2019). While there have been some studies conducted around phishing and social engineering email attacks, there is very limited research on individuals' Business Email Compromise Detection (BECD) skills related to cyberattacks focused on financial transaction through social engineering tactics. In addition, the exponential increase utilization of mobile device in the workplace has greatly extended reach to employees beyond the traditional work hours and places where business communication is typically conducted (David Bieling Bohnstedt Ohly Robnagel Schmitt Steinmerz Stock-Homburg and Wacker 2014). Furthermore, corporate user training is an important factor in BEC mitigation via user detection (Mansfield-Devine 2016). Moreover, there is a lack of employee

BEC awareness and lack of corporate procedures to mitigate BEC attacks (Jakobsson & Leddy, 2016). Therefore, it was imperative that this research study focused on the development and validation of a BEC detection measure of corporate users as well as the development of mobile user BEC detection awareness training module. This research utilized a cybersecurity expert panel to address two specific research questions:

RQ1: What are the cybersecurity experts' approved components of the experiment to measure BECD skills and its experimental protocol using the Delphi methodology?

RQ2: What are the cybersecurity experts' approved components of the mobile device users' BECD knowledge and awareness training program using the Delphi methodology?

This research study developed a new measure for BECD skills and utilized a panel of Cybersecurity experts leveraging the Delphi process to generate a consensus, which is the goal and requirement within the process to validate the measure (Dupuis Crossler and Endicott-Popovsky 2016).

LITERATURE REVIEW

Cyberattack methods in the Business Sector

Cybercriminals in the business sector are individuals or groups that conduct cyberattacks against corporations, governments, and other organizations primarily have malicious purposes for financial gain, theft of Intellectual Property (i.e. IP), or for destructive purposes (Hughes Bohl Ifran Margolese-Malin and Solorzano 2016). The global public Internet and advanced hacking methods also enable cybercriminals to conduct attacks from anywhere around the globe, while maintaining anonymity by making it very challenging to detect the source of the cyberattacks (Alazab 2015). The primary motive for cybercriminals to conduct an attack on an organization is for financial gain (Verizon 2016). Furthermore, the most utilized attack methods used by cybercriminals on corporate networks are email based cyberattacks, such as phishing and BEC social engineering attacks (Trustwave 2016). The increasing cyberattack complexity on corporate users utilizing malicious email-based attacks in the business segment, which warrants additional research in this on the users' ability to detect malicious email attacks (Stembert et al. 2015). Cybercriminals utilize email spoofing for BEC attacks to impersonate an executive corporate user request for money transfers in order to pressure the employees to comply with the request (Secureworks 2017). Therefore, additional research in corporate cybersecurity is needed to determine effective methods to mitigate email-based cyberattacks on corporations.

Evolution of Business Email Compromise Attacks

Phishing scams have long been used to gain sensitive information through email messages that seem to be trustworthy and authentic to the corporate users (Thakur Qui Gai and Ali 2015). Standard phishing attacks have attributed to over $1.6 billion in losses globally (Konradt Schilling and Werners 2016). The primary driver in conducting phishing attacks is for financial gain through exploiting system vulnerabilities and user unawareness (Gupta Tewari Jain and Agrawal 2016). Spear-phishing is increasingly targeting corporate users and corporations at an annual rate of 55% increase in 2015 from the previous year (Symantec 2016). Cybercriminals recognize the financial benefits of spear-phishing attacks on businesses, which by far exceed other phishing methods, therefore, the increase in spear-phishing attacks on the business segment (Sun Yu Lin and Tseng 2016). Thus, BEC attacks leverage phishing and spear-phishing attack methods to attain confidential information that is used to enable a successful BEC attack (FBI Internet Crime Complaint Center 2017). BEC attacks utilize phishing emails to impersonate corporate users in executive positions to attain information and request wire transfers from corporate users (Trend Micro 2017). Furthermore, the increase in mobile device use and mobile applications has led to an increase in mobile malware (Jang-Jaccard and Nepal, 2014). BEC attacks also utilize malware to attain information such as the victim's data, passwords, and financial account information (FBI Internet Crime Complaint Center 2017). Therefore, this research study utilized cybersecurity experts to develop the BEC detection measure components for corporate users' ability to detect BEC scams.

Business Email Compromise Defined

A BEC scam is a sophisticated cyberattack that is aimed at businesses that conduct wire transfers on a regular basis and leverage social engineering fraudulent emails to persuade an employee to conduct a wire transfer (FBI Internet Crime Complaint Center 2015). In recent years, corporate cyberattacks have quickly evolved toward email-based attacks that are posing a massive global threat to corporate cybersecurity, which has spiked a great interest in the research community (Gupta et al. 2016). More specifically, BEC attacks on companies and organizations of all sizes continue to grow, become more complex, and are significantly financially impacting (FBI 2017). The challenge with BEC attacks is that they have evolved into complex social engineering attacks to where security systems are limited in ability to detect these attacks and are more so dependent on the employees to be able to identify BEC attempts (Trend Micro 2017). One of the earlier victims of BEC attacks is Xoom, which transferred $31 million to a fraudulent account (Verizon 2016). Training and ensuring that corporate users are well informed are important factors in BEC attack mitigation as well as user detections skill (Mansfield-Devine 2016). Therefore, the current challenges and lack of success in mitigating BEC attacks warrant the need for additional research of the human attributes that are enabling BEC attack success.

This research study focused on corporate user detection of BEC attacks, which are sophisticated email-based cyberthreats that bring a new and complex financial risk to organizations (FBI 2017). Furthermore, expanding knowledge in the business segment around BEC attacks and developing corporate user training components not only contribute to the body of knowledge, but also for organizations mitigate financial losses due to BEC threats. Moreover, this research study included BEC awareness training module component development.

METHODOLOGY

This research study developed a BECD measure leveraging a cybersecurity expert panel review and analysis process utilizing the Delphi method. Furthermore, this research developed a BEC knowledge and awareness training module geared toward corporate professionals. The expert panel consisted of 30 cybersecurity experts who conducted the BEC measure review and analysis. The Delphi method is specifically designed for group communication and developed to avoid confrontation and achieve consensus across an expert panel (Ramim and Lichvar, 2014). Therefore, this research utilized the Delphi method to develop a valid instrument to measure BEC detection capabilities. To develop and validate the BEC detection (BECD) measure components, the research methodology process as shown in Figure 1 was conducted.

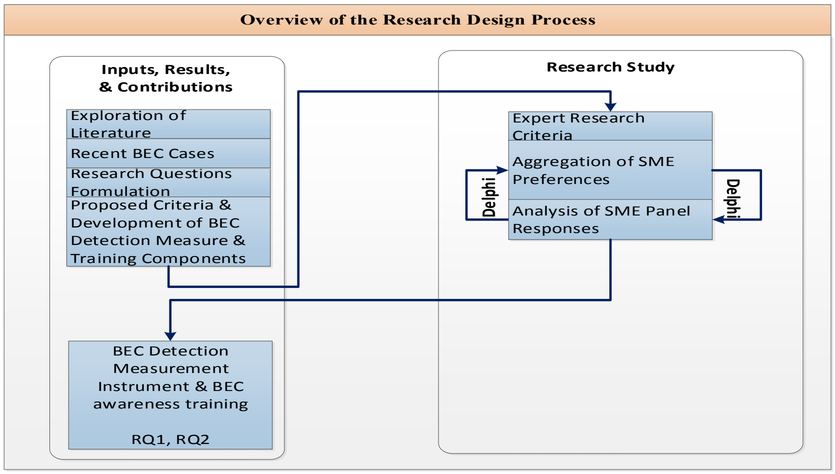

Overview of the Research Design Process
Inputs, Results, & Contributions
Exploration of Literature
Recent BEC Cases
Research Questions Formulation
Proposed Criteria & Development of BEC Detection Measure & Training Components
BEC Detection Measurement Instrument & BEC awareness training
RQ1, RQ2
Research Study
Expert Research Criteria
Aggregation of SME Preferences
Analysis of SME Panel Responses
Delphi
Delphi

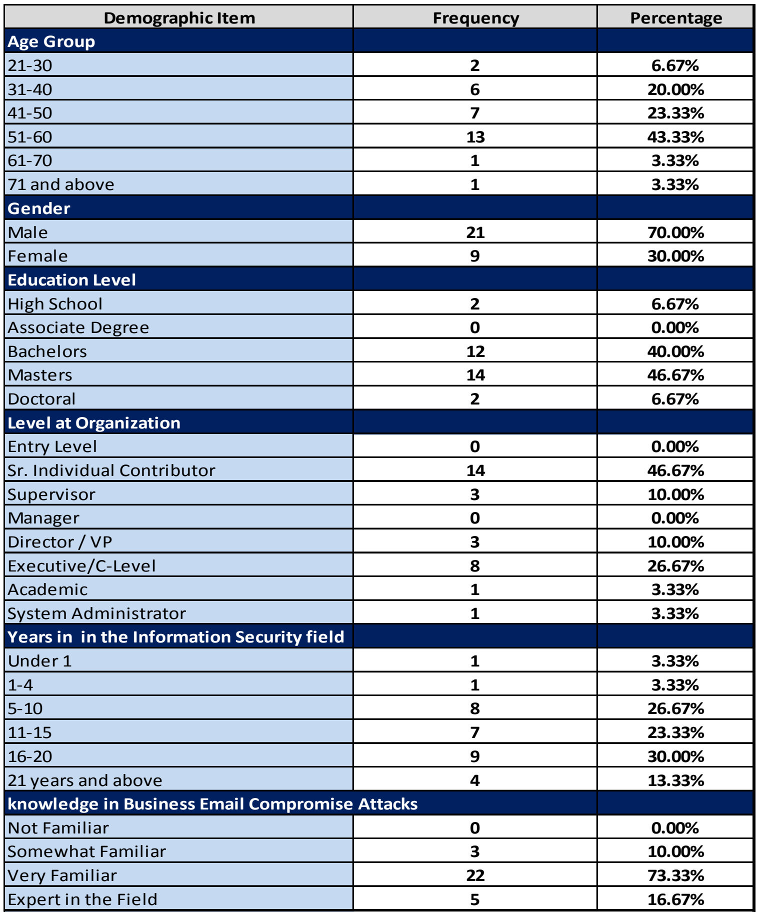
Figure 1: Research methodology Process overview

DATA ANALYSIS AND RESULTS

A panel of 42 cybersecurity experts was targeted with 30 experts responding. There were two Delphi rounds, which represents a 71% expert response rate. The Delphi method is a highly effective tool that and has a long history of accuracy and validity in research (Okoli, and Pawlowski, 2004). Moreover, a consensus threshold range of 87% to 97% was achieved for the measurement instrument and training module which deemed the Delphi process results above the standard and acceptable for the study.

Upon expert panel agreement to participate in this research study, the measurement instrument questions and components were distributed via anonymous online forms to the expert panel for modification, further development, and approval. There was a total of two sequential Delphi rounds conducted which were refined based on cybersecurity expert panel feedback. The cybersecurity expert panel indicated which components for the BEC detection measure and BEC awareness training module that should be included, provided their level of agreement via 7-point Likert scale, and asked for additional recommendations. The first Delphi round included capturing of cybersecurity expert panel demographics, BED detection measure components, and BEC awareness training module components. The second Delphi round consisted of the refined BEC detection measure components and training module components to provide validation. Consensus was achieved for all BEC detection measure components and training module components within the two Delphi rounds. In view of the above standard consensus achieved, no additional Delphi rounds were required. The cybersecurity expert panel feedback around the research components were analyzed and validated a high consensus on each component area. Table 1 indicates the descriptive Statistics of the expert panel.

Table 1. Descriptive Statistics of Cybersecurity Expert Panel (N=30)

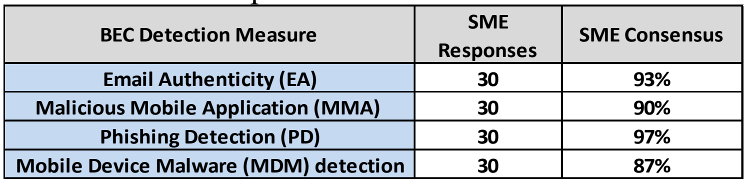


Demographic Item	Frequency	Percentage
Age Group		
21-30	2	6.67%
31-40	6	20.00%
41-50	7	23.33%
51-60	13	43.33%
61-70	1	3.33%
71 and above	1	3.33%
Gender		
Male	21	70.00%
Female	9	30.00%
Education Level		
High School	2	6.67%
Associate Degree	0	0.00%
Bachelors	12	40.00%
Masters	14	46.67%
Doctoral	2	6.67%
Level at Organization		
Entry Level	0	0.00%
Sr. Individual Contributor	14	46.67%
Supervisor	3	10.00%
Manager	0	0.00%
Director / VP	3	10.00%
Executive/C-Level	8	26.67%
Academic	1	3.33%
System Administrator	1	3.33%
Years in in the Information Security field		
Under 1	1	3.33%
1-4	1	3.33%
5-10	8	26.67%
11-15	7	23.33%
16-20	9	30.00%
21 years and above	4	13.33%
knowledge in Business Email Compromise Attacks		
Not Familiar	0	0.00%
Somewhat Familiar	3	10.00%
Very Familiar	22	73.33%
Expert in the Field	5	16.67%

Business Email Compromise Detection Measure Components

BEC scams are complex and sophisticated attached which are customized and comprised of multiple cyberattacks to ensure success (FBI 2017). With BEC attacks, cybercriminals impersonate a trusted colleague within the organization, such as the CEO and request that the targeted employee conduct a wire transfer in a fashion that seems to be a legitimate task (Jakobsson and Leddy 2016). BEC attacks utilize several forms of email configurations in order to successfully deploy the attack, such as a fake email account that could be passed off as a colleagues personal account, a closely mimicked domain alias of the organization that may pass as a legitimate corporate email account, or it may be an actual corporate email account where access was gained through other attacks such as malware to gain the credentials (Mansfield-Devine 2016). Therefore, this research study developed an instrument to measure BECD skills amongst corporate users. The focus of this research was on a BEC detection measure for corporate users in executive leadership roles such as Chief Executive Officers (CEO), Chief Financial Officers (CFO), and any corporate leader that utilizes mobile email communications and have authority to approve financial transfers to 3rd party vendors. BEC attacks are derived from spoofed of hacked email accounts where hackers use tactics such as malicious links, malware, and phishing emails to gain access to the victim's data (FBI 2017). Furthermore, mobile malware indicators include behaviors such as slow performance, reported text messages that were not sent by the mobile user, and the mobile device battery is draining quicker than in the past (Steinberg 2016). This research study found that there are four key components within the BEC detection measure and shown in Table 2.

Table 2. BEC Detection Measure Components



BEC Detection Measure	SME Responses	SME Consensus
Email Authenticity (EA)	30	93%
Malicious Mobile Application (MMA)	30	90%
Phishing Detection (PD)	30	97%
Mobile Device Malware (MDM) detection	30	87%

The email authenticity component refers to the corporate users' capability to recognize and identify the authenticity of their sent emails. The malicious mobile application detection refers to users' detection skill and familiarity with credible and malicious mobile applications. Phishing detection is the users' ability to detect credible and fraudulent incoming emails. Finally, the mobile device malware refers to malware indicators such as impacting the phone's performance, and data usage.

The results indicate the four key components which combined comprise the BECD measure as indicated in Table 2. The total BECD score indicates a range from a low BECD skill to an extremely high BECD skill amongst corporate mobile device users.

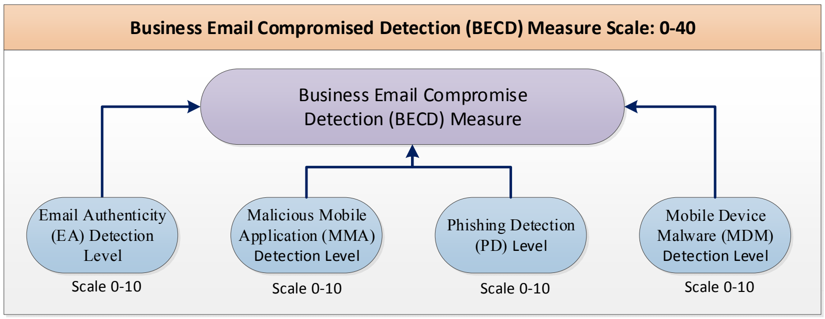

Business Email Compromised Detection (BECD) Measure Scale: 0-40
Business Email Compromise Detection (BECD) Measure
Email Authenticity (EA) Detection Level
Scale 0-10
Malicious Mobile Application (MMA) Detection Level
Scale 0-10
Phishing Detection (PD) Level
Scale 0-10
Mobile Device Malware (MDM) Detection Level
Scale 0-10

Figure 2: Research design for business email compromise measure

This research further found specific sub-components within phishing and mobile malware indicators. There is a lack of research around phishing email attacks within organizations as in the examination of corporate user behavior around social engineering attack detection (Flores and Ekstedt 2016). The phishing detection components found are indicated in Table 3 and the specific mobile malware detection components found are indicated in Table 4.

Table 3. Phishing detection components

Phishing Detection (PD)	SME Component Consensus
Requesting to fill in personal information.	87%
Suspicious, unrecognized URL, or URL mismatch	100%
The “From” address is an imitation of a legitimate address	97%
Pressure tactic to click and/or enter information (i.e. urgent matter, threatening emails, etc.)	87%
The mail contains suspicious or unexpected attachments	93%
The URL or link shows as unsecure (http://)	87%
Poor spelling and grammer	90%
Mis-spelled or slightly different URL or email address domain than expected on email	93%
Email from unknown sender making big promises	93%
Request for money for business reason (i.e. expense, bill payment, etc.)	97%
Suspicious Email claiming to be from a government agency	87%
Password reset email from a known social network or financial institution	100%

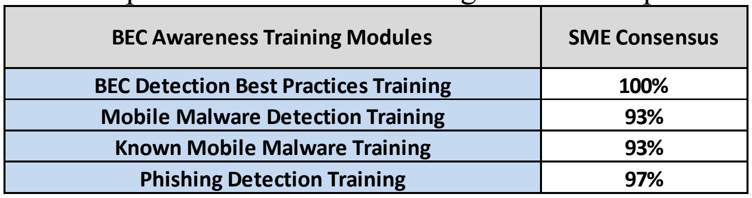
Table 4. Mobile device malware components

Mobile Device Malware (MDM)	SME Component Consensus
Mobile Device performance is slow	87%
Battery drains quickly	97%
Screen Freezes	93%
Spike in data usage	97%
Popups Ads	87%
Wifi/Bluetooth turn on automatically	87%
Phone overheats	100%
Unexplained phone charges	90%
Unrecognized Outgoing calls/texts	87%
Application crashes	100%

Business Email Compromise Awareness Training Module

Current cybersecurity training programs within corporations are inadequate and do not detect nor prevent BEC attacks (Zweighaft 2017). Moreover, conducting training around email attacks has shown to improve users' susceptibility to become victims (Sheng Holbrook Kumaraguru Cranor and Downs 2010). Therefore, developing a training module was a key focus of this research study. The training components are depicted in Table 5.

Table 5. Business email compromise awareness training module components



BEC Awareness Training Modules	SME Consensus
BEC Detection Best Practices Training	100%
Mobile Malware Detection Training	93%
Known Mobile Malware Training	93%
Phishing Detection Training	97%

CONCLUSIONS AND DISCUSSIONS

The main goal of this research study was to determine the cybersecurity expert panel approved components for measuring business email compromise detection capabilities. Furthermore, this study aimed to develop an expert approved BEC awareness training module for corporate professionals that conduct and have approving authority for wire transfers. These users fall under the BEC CEO scheme where the CEO or other business executive's email account is either hacked or spoofed and leveraging that account to request a wire transfer to the fraudulent account (Anderson 2016). The BECD measure instrument was developed utilizing cybersecurity experts via the Delphi process. The Delphi method is an effective approach in achieving an expert panel consensus in designing a measurement instrument (Ramim and Lichvar 2014). The strongest BEC defenses are having strong user procedures and policies in place (Mansfield-Devine 2016). Insight into the human aspects that influence the detection of BEC attacks can greatly help reduce risk of massive financial losses for organizations.

FUTURE RESEARCH

The continued growth of BEC attacks is an indicator that current research methodologies are insufficient and affirm that additional research is needed (Wilkerson 2017). The literature review determined that there is a very limited research in the area of BEC attacks. In cybersecurity within the business sector, there is limited research around the employees' personality characteristics, which are critical components in managing cyberattack risk and must be taken into consideration by organizations (Safa Sookhak Solms Furnell Ghani and Herawan 2015). In addition to user personalities, the user attention span levels are impacting their response to cybersecurity threats (Neupane Saxena Maximo and Kana 2016). Decreased attention span has been found in numerous studies to gear user attention away from suspicious fraud factors in phishing attacks, but rather on the urgency of the response (Greitzer Strozer Moore Mundie and Cowley 2014). Therefore, this research study can be further expanded by adding additional user characteristics such as personality attributes and attention span.

REFERENCES

Alazab, M. (2015). Profiling and classifying the behavior of malicious codes. *Journal of Systems and Software, 100*, 91-102. doi: 10.1016/j.jss.2014.10.031

Anderson, V. D. (2016, March 29). FBI warns of rise in schemes targeting businesses and online fraud of financial officers and individuals. *FBI Cleveland News*. Retrieved from https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals

Bendovschi, A. (2015). Cyber-attacks – Trends, patterns and security countermeasures. *Procedia Economics and Finance, 28*, 24-31.

David, K., Bieling, G., Bohnstedt, S. J., Ohly, S., Robnagel, A., Schmitt, A., Steinmerz, R., Stock-Homburg, R., and Wacker, A. (2014). Balancing the online life: Mobile usage scenarios and strategies for a new communication paradigm. *Institute of Electrical and Electronic Engineers Computer Vehicular Technology Magazine*, *9*(3), 72-79. doi: 10.1109/MVT.2014.2333763

Deshmukh, P., Shelar, M., and Kulkarni, N. (2014). Detecting of targeted malicious email. *Institute of Electrical and Electronic Engineers Global Conference on Wireless Computing and Networking*, 199-202. doi: 10.1109/GCWCN.2014.7030878

Dupuis, M. J., Crossler, R. E., and Endicott-Popovsky, B. (2016). Measuring the human factor in information security and privacy. *Institute of Electrical and Electronic Engineers Hawaii International Conference on System Sciences*, 3676-3685. doi: 10.1109/HICSS.2016.459

Federal Bureau of Investigations. (2015). *Business e-mail compromise*. Retrieved from: https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

Federal Bureau of Investigations. (2017, February 27). *Business e-mail: Cyber-enabled financial fraud on the rise globally*. Retrieved from https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Federal Bureau of Investigations Internet Crime Complaint Center. (2015). *Business e-mail* *compromise public service announcement*. Retrieved from: https://www.ic3.gov/media/2015/150827-1.aspx

Federal Bureau of Investigations Internet Crime Complaint Center. (2019). *Business Email Compromise The $26 Billion Scam*. Retrieved from: https://www.ic3.gov/media/2019/190910.aspx

Flores, W. R., and Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture awareness. *Journal of Computers and Security, 59*, 26-44. doi: 10.1016/j.cose.2016.01.004

Furnell, S., Millet, K., and Papadaki, M. (2019). Fifteen years of phishing: Can technology save us? *Journal of Computer Fraud and Security, 7*, 11-16. doi: https://doi.org/10.1016/S1361-3723(19)30074-0

Greitzer, F. L., Strozer, S. C., Moore, A. P., Mundie, D., and Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. *Institute of Electrical and Electronic Engineers Conference on Security and Privacy,* 236-250. doi: 10.1109/SPW.2014.39

Gupta, B. B., Tewari, A., Jain, A. K., and Agrawal, D. P. (2016). Fighting against phishing attacks: state of the art and future challenges. *Journal of Neural Computing and Applications,* 1-26. doi: 10.1007/s00521-016-2275-y

Hughes, B. B., Bohl, D., Ifran, M., Margolese-Malin, E., and Solorzano, J. R. (2016). ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. *Journal of Technological Forecasting and Social Change,* 1-14. doi: 10.1016/j.techfore.2016.09.027

Jakobsson, M., and Leddy, W. (2016). Could you fall for a scam? Spam filters are passe. What we need is software that unmasks fraudsters. *Institute of Electrical and Electronic Engineers Spectrum Magazine, 53*(5), 40-55. doi: 10.1109/MSPEC.2016.7459118

Jang-Jaccard, J., and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. doi: 10.1016/j.jcss.2014.02.005

Konradt, C., Schilling, A., and Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Journal of Computers and Security, 58*, 39-46. doi: 10.1016/j.cose.2015.12.001

Mansfield-Devine, S. (2016). The imitation game: How business email compromise scams are robbing organizations. *Journal of Computer Fraud and Security, 11*, 5-10. doi: 10.1016/S1361-3723(16)30089-6

Nandi, A. K., Medal, H. R., and Vadlamani, S. (2016). Interdicting attack graphs to predict organizations from cyberattacks: A bi-level defender-attacker model. *Journal of Computers and Operations Research,* 24-31. doi: 10.1016/j.cor.2016.05.005

Neupane, A., Saxena, N., Maximo, J. O., and Kana, R. (2016). Neural markers of cybersecurity: An fMR study of phishing and malware warnings. *Institute of Electrical and Electronic Engineers Journal of Transactions on Information Forensics and Security, 11*(9), 1970-1983. doi: 10.1109/TIFS.2016.2566265

Okoli, C., and Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design, considerations and applications. *Journal of Information and Management, 42*(1), 15-29. doi: 10.1016/j.im.2003.11.002

Ramim, M. M., and Lichvar, B. T. (2014). Elicit expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management, 2*(1), 122-136.

Roumani, M. A., Fung, C. C., and Choejey, P. (2015). Assessing economic impact due to cyber attacks with system dynamics. *Institute of Electrical and Electronic Engineers International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology,* 1-6. doi: 10.1109/ECTICon.2015.7207084

Safa, N. S., Sookhak, M., Solms, E.V., Furnell, S., Ghani, N. A., and Herawan, T. (2015). Information security conscious care behavior in organizations. *Journal of Computers and Security, 53*, 65-78. doi: 10.1016/j.cose.2015.05.012

Secureworks. (2017), *2017 State of cybercrime report: Exposing the threats, techniques, and markets that fuel the economy of cybercriminals*. Retrieved from: https://www.secureworks.com/~/media/Files/US/Reports/SecureworksSECO1150N2017StateofCybercrimeReport.ashx

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *International Association for Computer Machinery Conference on Human Factors in Computer Systems,* 373-382. doi: 10.1145/1753326.1753383

Steinberg, J. (2016, November 1). 14 signs your smartphone or tablet has been hacked. *Inc Magazine*. Retrieved from https://www.inc.com/joseph-steinberg/14-signs-your-smartphone-or-tablet-has-been-hacked.html

Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., and Jansen, F. (2015). A study preventing email (spear) phishing by enabling human intelligence. *Institute of Electrical and Electronic Engineers International Conference on Intelligence and Security Informatics,* 113-120. doi: 10.1109/EISIC.2015.38

Symantec. (2016), *Internet security threat report*. Retrieved from: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Thakur, K., Qui, M., Gai, K., and Ali, M. L. (2015). An investigation on cyber security threats and security models. *Institute of Electrical and Electronic Engineers International Conference on Cyber Security and Cloud Computing,* 307-311. doi: 10.1109/CSCloud.2015.71

Trend Micro. (2017), *2017 Midyear security roundup:The cost of compromise*. Retrieved from: https://documents.trendmicro.com/assets/rpt/rpt-2017-Midyear-Security-Roundup-The-Cost-of-Compromise.pdf

Trustwave. (2016), *Trustwave global security report*. Retrieved from: https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf

Verizon. (2016), *Data breach investigations report*. Retrieved from: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Wilkerson, S., Levy, Y., Kiper, J.R., Snyder, M. (2017). Toward a development of a social engineering exposure index (SEXI) using publicly available personal information. *2017 Kennesaw State University Conference on Cybersecurity Education, Research and Practice,* 1-9.

Zweighaft, D. (2017). Business email compromise and executive impersonations: are financial institutions exposed? *Journal of Investment Compliance, 18*(1), 1-7. doi: 10.1108/JOIC-02-2017-0001