International Journal of Human-Computer Studies 120 (2018) 1–13

Contents lists available at ScienceDirect

International Journal of Human-Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

Exploring susceptibility to phishing in the workplace

Emma J. Williams*, Joanne Hinds, Adam N. Joinson

School of Management, University of Bath, Claverton Down, Bath BA2 7AY, UK

ARTICLE INFO

Keywords:
Phishing
Organisational behavior
Human factors
Cyber security
Employee susceptibility
Social engineering

ABSTRACT

Phishing emails provide a means to infiltrate the technical systems of organisations by encouraging employees to click on malicious links or attachments. Despite the use of awareness campaigns and phishing simulations, employees remain vulnerable to phishing emails. The present research uses a mixed methods approach to explore employee susceptibility to targeted phishing emails, known as spear phishing. In study one, nine spear phishing simulation emails sent to 62,000 employees over a six-week period were rated according to the presence of authority and urgency influence techniques. Results demonstrated that the presence of authority cues increased the likelihood that a user would click a suspicious link contained in an email. In study two, six focus groups were conducted in a second organisation to explore whether additional factors within the work environment impact employee susceptibility to spear phishing. We discuss these factors in relation to current theoretical approaches and provide implications for user communities.

1. Introduction

Organisations are increasingly under threat from attackers attempting to infiltrate their computer systems by exploiting the behaviour of human users (Sasse et al., 2001). One means by which this can be achieved is via targeted, fraudulent emails, which aim to persuade employees to click on malicious links, download malicious attachments or transfer organisational funds or other sensitive information. This practice is commonly known as spear phishing (Workman, 2008). A 2016 Cyber Incident Report (Verizon, 2016) highlighted that over 2,000 organisations experienced a data breach in 2015, with the highest number experienced by organisations in the financial sector (a total number of 795). This same report also showed that approximately 1 in 10 employees of such organisations clicked on links or opened attachments contained within sanctioned phishing email tests.

One way in which organisations attempt to raise awareness of spear phishing emails amongst their staff is through the use of simulated phishing tests. This involves the organisation sending simulated, targeted phishing emails to a number of employees and monitoring the resultant 'click-rate' (i.e., the proportion of employees who click on malicious links within the email). Such emails, whether sent as part of simulated phishing tests or by actual fraudsters, use a range of influence techniques to encourage people to respond quickly and without consideration. This includes instilling a sense of urgency or limited availability and exploiting compliance with authority figures (Atkins and Huang, 2013; Cialdini, 2007; Stajano and Wilson, 2011). Examples of influence techniques used in spear phishing emails are shown in Table 1. When such attacks are successful, they can result in substantial reputational damage, monetary losses or operational impacts for the organisation involved (e.g., Landesman, 2016; Piggin, 2016; Zetter, 2016). It is this threat that has contributed to the rise of anti-phishing training games, formal phishing simulation tests, and interface design initiatives to increase employee awareness and assist in the effective management of phishing risks within the workplace (Abawajy, 2014; Dodge et al., 2007).

Despite an increased focus on training and awareness approaches, a 2016 report produced by security training firm PhishMe highlighted that employees continue to be vulnerable to phishing attacks, with an average response rate of approximately 20% (Computer Fraud and Security, 2016; PhishMe, 2016). This includes responses to both spear phishing and generic phishing emails. This report, which was based on the analysis of over 8 million simulated phishing emails, also highlighted that 67% of employees who respond to simulated phishing attacks are repeat victims and therefore likely to respond to phishing emails more than once. The continuing vulnerability of many organisations to phishing attacks has led the UK National Cyber Security Centre to recently release specific guidance for organisations regarding how they can defend themselves from the phishing threat (NCSC, 2018a).

The hierarchical nature of many workplaces and employees' limited time means that they are likely to be particularly susceptible to the authority and urgency influence techniques highlighted by

* Corresponding author at: School of Experimental Psychology, University of Bristol, Priory Road, Bristol BS8 1TU, UK.
E-mail address: emma.williams@bristol.ac.uk (E.J. Williams).

https://doi.org/10.1016/j.ijhcs.2018.06.004
Received 23 June 2017; Received in revised form 23 April 2018; Accepted 30 June 2018

Table 1
Example influence techniques that occur in phishing emails.

Technique	Description
Authority	Claims to come from an individual or institution that represents an authority figure.
Urgency	States that the receiver has a limited time to respond.
Reciprocity	Claims to provide some form of favour to the recipient.
Social proof	Suggests that other people have responded to the email.
Reward	Claims to provide the receiver with a potential reward if they respond.
Loss	Claims that the receiver will suffer some form of loss if they fail to respond.
Scarcity	Suggests that an offer or opportunity is limited in some way (e.g., for the first 10 respondents).

Cialdini (2007) and Stajano and Wilson (2011). Elements of the particular work context in which a spear phishing email is received (such as receiving an urgent request whilst being particularly busy or distracted) are also likely to exacerbate susceptibility. However, difficulties in accessing data related to susceptibility within workplace settings have severely limited current understanding of these factors. Therefore, there is much to be gained from investigating the role of both influence techniques and work-related contextual factors using applied data sources. This will not only aid theoretical development, but also assist in advancing practical interventions. The present paper uses data from two organisations that routinely handle sensitive information to address this current limitation; using a novel approach that enables existing theoretical concepts to be considered and new ones to be identified in relation to applied workplace settings.

The paper is structured as follows. First, we briefly consider current theoretical approaches and research findings relevant to susceptibility to spear phishing emails. We then present two studies conducted in organisational settings. In Study One, we take a novel approach to the examination of message-related factors (specifically, the presence of authority and urgency influence techniques) by examining historic data from simulated phishing tests within organisation A. In Study Two, we undertake a qualitative exploration of wider susceptibility factors related to the individual recipient and the context that they are in (including how familiar they are with the message sender, whether they are expecting a particular communication, and their awareness of the potential risk of spear phishing) by exploring employee perceptions of susceptibility within the work environment using a focus group methodology in a second organisation (organisation B). Although Williams et al. (2017a) discuss the potential role of these various aspects on susceptibility to online influence in their theoretical review, there is limited empirical evidence to date. The current studies take a first step in addressing this gap. We conclude by considering these findings in relation to the potential expansion of current theories. We also consider potential contributions to practical applications, including interface design, employee training and awareness, and decision support systems.

1.1. Theoretical justification

Over the last decade, researchers have attempted to identify the primary factors that may impact individual susceptibility to phishing emails. This has led to the development and application of a range of theoretical frameworks, including the Integrated Information Processing Model of Phishing Susceptibility (IIPM; Vishwanath et al., 2011), the Suspicion, Cognition, and Automaticity Model (SCAM; Vishwanath et al., 2016), and Protection Motivation Theory (PMT; Rogers, 1975). Although these models show a degree of overlap, they have rarely been studied together, despite the fact that all of the highlighted elements are likely to influence susceptibility to spear phishing. For instance, PMT has been more commonly applied to generic security behaviour and examines individual perceptions of threat and perceived ability to manage such threats. Conversely, the SCAM incorporates individual knowledge, beliefs and habits in relation to phishing susceptibility specifically. Finally, the IIPM focuses primarily on the information processing style that is used when a phishing email is encountered. These models have also not been extensively studied using organisational data. Exploring the role of all of these aspects within organisational settings provides a unique opportunity to understand the full range of factors that may influence susceptibility in the workplace. We further consider each of these models in relation to our study aims below.

1.1.1. The integrated information processing model of phishing susceptibility (IPPM)

The IPPM suggests that the likelihood that an individual will respond to a phishing email is influenced by the content of the email, such as the influence techniques that it contains, the use and accuracy of email signatures, and the sender address (Vishwanath et al., 2011). Specifically, the model claims that people's limited attentional resources are monopolised by the presence of particular influence techniques such as urgency (e.g., an urgent deadline). This increases the likelihood that people will rely on relatively automatic forms of information processing (known as *heuristic* processing) when deciding how to respond and will not engage in more in-depth consideration of the legitimacy of the email (known as *systematic* processing: Eagly and Chaiken, 1993; Harrison et al., 2016a; Kahneman, 2011; Luo et al., 2013; Vishwanath et al., 2011; 2016). As a result, authenticity cues within the email (i.e., features a person uses to determine legitimacy), such as an incorrect sender address, are more likely to be overlooked.

The relative role of particular influence techniques in influencing individual susceptibility to phishing remains uncertain, however (Oliveira et al., 2017). For instance, when comparing participant responses to genuine, phishing and spear phishing emails that contained authority, scarcity or social proof influence techniques, Butavicius et al. (2015) found greater susceptibility to emails that contained authority cues. Williams et al. (2017b) also manipulated the presence of authority cues within fraudulent software updates whilst keeping the presence of urgency cues constant and found that participants were particularly susceptible to updates containing authority cues. However, in a field experiment where different phishing messages were sent to more than 2,600 participants, the presence of authority influence techniques was not found to increase click-rates (Wright et al., 2014). In their analysis of participants' self-reported reasons for responding to fraudulent updates, Williams et al. (2017a) further highlighted the role of other message-related cues, such as how familiar participants were with the particular update message (i.e., whether they had received similar messages before) and whether they were expecting a particular communication.

To our knowledge, the relative role of such influence techniques has yet to be explicitly examined within workplace settings. This is despite the fact that particular influence techniques may be differentially relevant, and therefore have different effects, in work contexts. Within study one, therefore, we explicitly investigate whether the presence of authority and urgency techniques influence employee susceptibility to simulated spear phishing emails within the workplace. We extend this in Study Two by examining employee discussions of the message-related factors that they report as making them more or less likely to respond to an email that they receive.

1.1.2. The suspicion, cognition and automaticity model (SCAM)

The SCAM claims that the extent to which heuristic processing strategies are used when evaluating emails varies according to characteristics of the individual recipient (Vishwanath et al., 2016). These differences primarily relate to individual beliefs regarding online risk (Barnett and Breakwell, 2001; Bromiley and Curley, 1992), which encompasses the degree of experience, efficacy, and subject-specific knowledge that people have (Downs et al., 2006; Canfield et al., 2016;