Decision Support Systems xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Decision Support Systems

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

# Do phishing alerts impact global corporations? A firm value analysis

Indranil Bose [a,*], Alvin Chung Man Leung [b,1]

[a] Indian Institute of Management Calcutta, Diamond Harbour Road, Joka, Kolkata 700104, India
[b] Department of Information Systems, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong

ARTICLE INFO

*Article history:*
Received 1 May 2013
Received in revised form 15 April 2014
Accepted 22 April 2014
Available online xxxx

*Keywords:*
Abnormal returns
Event study
Financial holding companies
Firm value
Phishing
Trading volume

ABSTRACT

Phishing is a form of online identity theft that is increasingly becoming a global menace. In this research, we analyze the impact of phishing alerts released in public databases on the market value of global firms. Using a sample of 1942 phishing alerts related to 259 firms in 32 countries, we show that the release of each phishing alert leads to a statistically significant loss of market capitalization that is at least US$ 411 million for a firm. We propose a theoretical framework for analyzing the impact of threats on firm value, and determine that the negative investor reaction is strongly significant for alerts released in 2006–2007 and for those targeted to financial holding companies, and weakly significant for firms listed in the US. We derive and validate these results using a combination of event study, subsampling analysis, and cross-sectional regression analysis. Our research makes a contribution by providing a new model for conducting multi-country event studies. We also contribute to the information systems literature by quantifying the loss in market value caused by phishing, and provide compelling evidence to information security administrators of firms that urge them to adopt adequate countermeasures to prevent phishing attacks.



## 1. Introduction

"Cyber-crime has become a $105 billion business that now surpasses the value of the illegal drug trade worldwide." — David DeWalt, CEO of McAfee [67]

With an increasing number of Internet crimes, online security has become a major concern for the general public. Among various online frauds, phishing, "a form of social engineering in which an attacker attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization", is one of the biggest threats to the online community [50]. This online crime has grown tremendously in recent years. According to the Anti-Phishing Working Group (APWG) the number of phishing incidents has increased from 47,324 in the first half of 2008 to 126,697 in the second half of December 2009. Since its first appearance around 1995, phishing has spread all over the world affecting millions of customers and numerous firms. Fig. 1 shows how phishing attacks take place and various associated financial losses. The actual financial loss due to phishing attacks may be ten times more than the estimated numbers for direct loss due to the indirect and the opportunity loss inflicted by phishing — an estimate of which is unavailable in literature [41]. Indirect losses take the form of increased customer support to phishing victims as well as efforts of customers to deal with credit-rating agencies to prevent themselves from being blacklisted due to the attacks. According to Meg Whitman, the former CEO of eBay, phishing has caused deterioration of trust of online customers and impaired e-commerce [10]. Her concern about opportunity loss is supported by the fact that the rate of opening of legitimate emails has dropped by 20% [9], and in a survey 89% of the respondents expressed concern about phishing attacks [79].

Motivated by the lack of research on the indirect and opportunity loss of phishing and particularly the lack of analysis of the impact of phishing on a worldwide basis, we embarked on analyzing the impact of phishing on the market value of firms. We collected data on phishing alerts targeted to global firms that were released by anti-phishing organizations. These alerts either included emails that were being sent to customers of public companies or notifications about fake websites that were being set up to lure customers. Using the event study method, we determined the impact of such alerts on the market value of global public firms by evaluating the change in their stock prices and trading volume after the release of the alerts. We also determined the various factors that influenced the impact.

Phishing has been a subject of intense research recently. The social and legal responsibilities of phishing were studied by researchers [7,88]. Technical research on phishing included development of anti-phishing tools such as AntiPhish, which is a browser extension that generates warning messages when users give away personal information to fake websites [58], and BogusBiter, which is a browser extension that feeds fake user information to phishing websites [89]. In business focused research on phishing, researchers analyzed anti-phishing preparedness of Hong Kong banks [8] and identified antecedents for the

* Corresponding author. Tel.: +91 33 2467 8300; fax: +91 33 2467 8062.
*E-mail addresses:* indranil_bose@yahoo.com (I. Bose), aleung@utexas.edu (A.C.M. Leung).
[1] Tel.: +852 3442 8521; fax: +852 3442 0370.

http://dx.doi.org/10.1016/j.dss.2014.04.006
0167-9236/

Please cite this article as: I. Bose, A.C.M. Leung, Do phishing alerts impact global corporations? A firm value analysis, Decision Support Systems (2014), http://dx.doi.org/10.1016/j.dss.2014.04.006

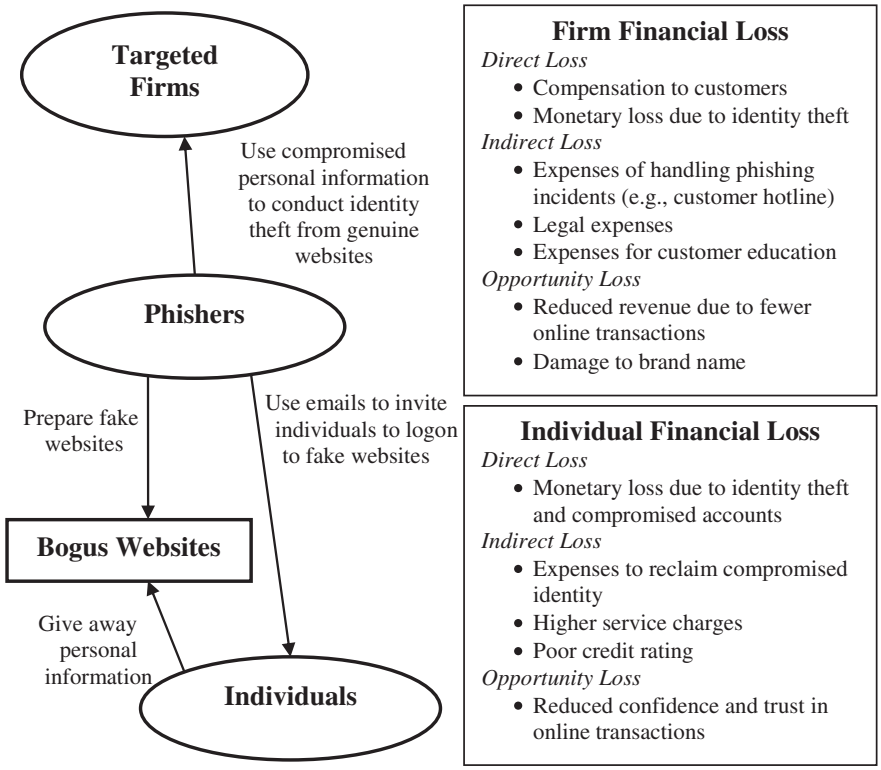


**Fig. 1.** Phishing attacks and their impacts on firms and individuals.

severity of phishing attacks [20]. Experimental studies discovered that user related behavioral and dispositional factors and phisher related social relationship mining skills led to success of phishing [49]. In summary, phishing has spurred enormous interest in academia and many anti-phishing tools and behavioral studies were conducted. Nevertheless, do industrial practitioners believe that the benefits of anti-phishing products justify the cost of adoption? This paper aims at providing a reasonable estimation of the loss in market value due to phishing. Through this study, we hope to arouse the awareness of managers to phishing and encourage them to adopt appropriate anti-phishing tools.

Our research is similar to past research conducted on information security breaches and their market impact. Using an event study, researchers showed that mishandling of confidential information [12], unauthorized access, hacking, denial of service (DoS), website vandalism [14], online credit cards thefts, website defacements [35], data breaches [36], and security breaches related to loss of integrity [52] caused a significant negative impact. The online nature of firms and tools used for attacks influenced the impact on firm value [2]. Prior research also reported negative but insignificant market reaction to DoS attacks [45]. Virus attacks resulted in contradictory positive and insignificant returns [46] as well as negative and insignificant returns [47] when different datasets were used.

The past research on the impact of security breaches examined only US firms. But there is no denying that security breaches in general and phishing attacks in particular are a global phenomenon. The insignificant market reaction observed in some prior studies could be due to the non-global nature of the research. Past research focused on discovering the link between security attacks and financial loss has often grouped various types of security breaches together [12,52]. Although DoS attacks and virus attacks have been studied separately [35,45,46], the impact of phishing on market value has not caught the attention of researchers. Phishing is a menace in its own right, and is different from other security breaches such as vandalism, DoS, and hacking. Those attacks are company oriented, and reveal the weakness of corporate security. On the contrary, phishing is customer oriented, and affects the perception of the customers about the targeted firm. This unique nature of phishing as a security breach motivates us to study its impact on global firms using 1942 alerts from 259 firms belonging to 32 countries. We also observe the lack of a theoretical framework in extant literature for studying the consequences of security breaches like phishing. We propose a risk-components based framework that explains why phishing causes a negative impact on firm value, and identifies factors at the firm, industry, country, and temporal levels that moderate the impact. Since our research involves firms from multiple countries, we improve on the traditional Capital Asset Pricing Model (CAPM) based event study method commonly used in Information Systems (IS) research, by proposing a refined asset pricing model that combines the Fama–French three factor model with the Fama–French international model, and is able to explain the risk in the cross-sectional abnormal return of global firms better. We conduct subsampling and cross-sectional regression to identify the significant moderating factors. Our results show that phishing alerts create statistically significant negative impact on stock prices and trading volume and lead to a loss of market capitalization that is at least US$ 411 million per alert. The market reaction becomes more pronounced for phishing alerts released in 2006–07 and for alerts targeted to financial holding companies. This research contributes to the literature on information security by quantifying the loss in market value caused by phishing, and providing hard evidence to security administrators to encourage adoption of adequate countermeasures to prevent phishing.

## 2. Theoretical framework

Our proposed framework for assessing the impact of security risks on market value of firms is shown in Fig. 2. According to Drucker, "risk is inherent to the commitment of present resources to future expectations" [27]. To model risk for a firm, we adapt the idea of risk-components proposed by Crockford [22]. The first component of risk is threats that can disrupt the functioning of an organization.

Please cite this article as: I. Bose, A.C.M. Leung, Do phishing alerts impact global corporations? A firm value analysis, Decision Support Systems (2014), http://dx.doi.org/10.1016/j.dss.2014.04.006