Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2008 Proceedings

International Conference on Information Systems (ICIS)

2008

# Indirect Financial Loss of Phishing to Global Market

Alvin C.M. Leung
*The University of Hong Kong*, alvinleung@business.hku.hk

Indranil Bose
*The University of Hong Kong*, bose@business.hku.hk

# INDIRECT FINANCIAL LOSS OF PHISHING TO GLOBAL MARKET

*Etude mondiale sur les pertes financières indirectes dues au hameçonnage*

*Completed Research Paper*

**Alvin C. M. Leung**
The University of Hong Kong
Room 730, Meng Wah Complex,
The University of Hong Kong,
Pokfulam Road, Hong Kong SAR, China
alvinleung@business.hku.hk

**Indranil Bose**
The University of Hong Kong
Room 615, Meng Wah Complex,
The University of Hong Kong,
Pokfulam Road, Hong Kong SAR, China
bose@business.hku.hk

## Abstract

*This research studies the indirect financial impact of phishing announcements on firm value. Using about 3,000 phishing announcements, we showed that phishing has a significantly negative impact on firms regardless of their size. We also discovered that place of incorporation, type of ownership, industry, and time are significant factors exacerbating the impact. Our research findings may give some insights to industrial practitioners about attitude of investors towards phishing. Compared to other similar event studies, our research has also made several significant breakthroughs. Firstly, we used the largest data set ever in prior event studies. Secondly, our research is the first to analyze global phenomena concerning phishing. Thirdly, we enhanced the robustness of a regression model by introducing the criterion of selection of best fit market index based on R square. We believe that our research can add value to the literature in the subjects of phishing research and event studies.*

**Keywords:** Phishing, Indirect Financial Impact, Information Security, Economics, Finance, Event Studies

## *Résumé*

*Cette étude pionnière porte sur l'impact financier indirect subi par les entreprises suite à des annonces de hameçonnage ("phishing"). Une enquête basée sur près de 3000 annonces de hameçonnage dans le monde nous a permis de montrer que le hameçonnage a un impact négatif considérable sur les entreprises, quelle que soit leur taille.*


# Introduction

Phishing, which is a kind of online identity theft, has existed for about 13 years with the first AOL theft incident occurring in 1995 (James 2005). Despite a short history, the increase in occurrence of these attacks has been tremendous. According to the Anti-Phishing Working Group, the number of phishing incidents increased exponentially from 8829 in December 2004 to 25328 in December 2007, with a rate of increase of 186.9% (APWG 2005; APWG 2008). At present about 58% of corporate Internet users receive at least one phishing email daily (M2 Presswire 2006) and it is estimated that at least 2 million people have released sensitive personal information in phishing incidents (Kirda and Kruegel 2005).

Since the appearance of phishing, the techniques have evolved from plain emails purportedly coming from legitimate sender asking for personal information, to more sophisticated methods such as emails accompanying professionally made fraudulent Web sites. More recently, Pharming, which hijacks Domain Name Servers to redirect request from a genuine Web site to a spoof one, causes turmoil to the society (Jakobsson 2005). Making use of the latest technologies, techniques such as Smishing, which is a phishing attack using short message service (SMS), and Vishing, which is an attack using voice over IP (VoIP), have emerged (Choo et al. 2007). Online identity theft has also spread from the US to countries all over the world. Phishing incidents have been reported in 6 continents although those in US remain the majority. It was estimated that in 2004 alone, the financial loss was US$1.2 billion (Geer 2005).

As the financial loss is huge, many concerned companies have established various anti-phishing measures. Deutsche Postbank has implemented electronic signatures to facilitate authentication of legitimate company emails (Libbenga 2006). Bank of America has launched SiteKey to add a second layer of authentication to better protect customers against identity theft (Nowell 2005). Governments worldwide have passed laws or ordinances to safeguard the general public, for instance, Identity Theft and Assumption Deterrence Act of US and Data Protection Directive of European Union (Bose and Leung 2007). With strong advocacy of anti-phishing from both industries and governments, the awareness of customers towards phishing has been heightened.

However, with the increasing number of phishing incidents, customers' confidence over electronic commerce has faded. In a consumer study conducted by Cyota, it was found that among 650 bank account holders, 75% relinquished the habit of online shopping due to the threat of phishing (Cardline 2004). Also, this anxiety has reduced the rate of opening legitimate email by 20 to 30% as reflected in a study of MarketingSherpa (Brandt 2005). Obviously, the indirect cost of e-commerce companies due to phishing is enormous. Currently, the estimated financial loss due to phishing is based on consumer surveys and the expected loss of revenue generated by e-commerce companies as a result of phishing. The variability of the surveys may be too subjective to give an accurate estimation. With a motivation towards quantifying the amount of indirect cost, we instigated this research with hope to give more concrete evidence that phishing hurts global e-commerce markets. Using an event study methodology, which is a robust method proven in many business disciplines, we intend to enumerate the indirect financial loss of market value due to phishing and arouse the awareness of industrial practitioners towards the better protection of customers against such online identity theft.

The rest of the paper is organized as follows. In the second section, we discuss relevant research studies in the fields of phishing research and information security. We identify the limitations of current research and show how our research can bridge the gap. In the third and fourth sections, we outline our research hypotheses and methodology. We show how we derive our research hypotheses and develop a more robust step in development of a regression model in our research methodology, which may contribute to existing literature in the field of event study. Finally, the implication of our research is drawn and interesting phenomena are discussed.

## Literature Review

Although phishing has been around for 13 years, research in this area is limited and mainly focused on technical research and phenomenological study. The former refers to technical innovations to safeguard customers against phishing attacks, for instance, Dynamic Security Skin (Dhamija and Tygar 2005), Web Wallet (Wu et al. 2006), Trust Bar (Herzberg and Gbara 2004), and Anti-Phish (Kirda and Kruegel 2005). The latter diagnoses the critical success factors of phishing attacks. The identified factors include social engineering skills, lack of knowledge, visual deception, and lack of attentiveness to detail (Dhamija and Tygar 2005; Jagatic et al. 2006). To the best of our knowledge, there is no other research study analyzing economic impacts of phishing. Our knowledge of economic loss is only based on actual financial loss in certain reported phishing incidents and estimation based on consumer surveys. However, those figures may not be an accurate reflection of reality. The estimated US$ 1 million financial loss due to phishing may be just one tenth of the real problem (Goth 2005). Some indirect financial loss, for instance, loss of future revenue due to lack of confidence of customers and damage of company brand, has not been considered. It is expected that indirect financial loss may be even more than the reported financial loss. This motivated us to conduct a more thorough analysis to investigate the economic impact of phishing on firm value.

In the field of information security, though not directly related to phishing, several research studies have been conducted on the economic impact of other security threats on firm value. Event study methodology, which has been proven to be a robust methodology in various disciplines from accounting and finance to management information systems, has been widely adopted. The summary of main findings of relevant literatures is as shown in Table 1.

**Table 1. Literature Review of Information Security Related Event Studies**

| Area of Study | Time Period | Number of Events | CAR |
|---|---|---|---|
| Impact of personal information security breaches on firm value (Campbell et al. 2003) | 1995-2000 | 43 | -5.5% * |
| Impact of information security breaches on firm value (Kannan et al. 2007) | 1997-2003 | 72 | -3.2% * |
| Impact of internet security breaches on firm value (Cavusoglu et al. 2004) | 1998-2000 | 66 | -2.1% * |
| Impact of denial of service attacks on firm value (Hovav and D'Arcy 2003) | 1998-2002 | 23 | [-90.3% , 62.1%] |
| Impact of software vulnerabilities on firm value (Telang and Wattal 2007) | 1999-2004 | 147 | -0.6% * |
| Impact of data breaches on firm value (Acquisti et al. 2006) | 2000-2005 | 79 | -0.6% * |
| Impact of SPAM on penny stocks (Bohme and Holz 2006) | 2004-2006 | 152 | +1.7% * |

*Significant at the 10% or less confidence level

The result of prior studies on information security shows that security threats in general have a negative impact on market value of target companies, especially, leakage of privacy data and breaches of information security. This may indicate that phishing, a type of security threat, may also pose a negative impact on market price. Nevertheless, the amount of financial loss due to phishing may not be accurately estimated in prior studies. A thorough analysis is necessary to obtain the answer. Also, one of the limitations of prior studies is that the subjects of the research are all US companies. As regional factors may dominate the research results, the universal phenomenon cannot be accurately determined on the basis of regional data.

Furthermore, the sample size of the research is not large enough in some prior studies. In the study of denial of service attack, insignificant results were obtained due to small sample size. Also, some research studies adopted a scope too wide for pinpointing a specific type of security threat. In study on breaches of information security, the

scope covered everything from data leakage to service availability. The impact could not adequately explain the influence of each individual information security breach on stock price. Moreover, in some research studies on thinly traded stocks, stocks that were listed on Pink Sheet and OTC were used. The robustness of the research studies is questionable as such stocks are extremely volatile. Nevertheless, prior research in the area of information security adds strong motivation towards conducting our research and foreshadows some of our research results.

In this research study, we bridged the literature gaps of both phishing research and information security. Our study is the first study on the economic impact of phishing on market value. The result can help quantify indirect financial loss due to identity theft. Secondly, our research data included worldwide phishing announcements and thus we were able to minimize the regional factors and more accurately suggest the extent of universal phenomena within this subject. Thirdly, our research sample size was the largest of all event studies in the field of management information systems. Therefore, our research should give rise to more robust findings. Also, we strictly followed the conventional event study methodology and eliminated any thinly traded stocks. Furthermore we refined the event study methodology by including the selection of the available best regression model. This enhanced the reliability of our research findings.

## Research Hypotheses

The motive of this research is to analyze the overall impact of phishing announcements on the market value of e-commerce companies. The research hypotheses are outlined in this section.

Phishing poses a threat to both e-commerce companies and their customers. Not only does it cause direct financial impact to the customers, but also hurts the brand image of the target companies because the occurrence of phishing implicitly reveals that the anti-phishing strategies are not adequate enough to deter the crime and thus causes financial loss to customers. Such attacks may shatter the confidence of customers in using the service provided by the companies. As a result, it is expected that future revenue of the firm may be lowered. From a rational investor's perspective, if other factors remain unchanged, it is better to sell the stocks of phishing targeted companies because the appearance of phishing announcements may expose the weaknesses of corporate information security and foreshadow poor performance in retaining existing customers. Therefore, it is expected that negative impacts on the market value of companies may emerge. Hypothesis 1 is conceived below. This conforms to the earlier studies on information security that phishing, which is a type of security threat, may pose a negative impact on market value.

H1: Phishing announcements have a negative impact on firm value regardless of firm size

The negative impact of phishing on market value may rely on the perception of investors, who associate phishing attacks with weak information security. Therefore, people who are more knowledgeable about phishing may have a stronger perception concerning the matter. It is conjectured that developed countries, where people are more accustomed to electronic services, may have stronger perceptions about the association and thus penalize the companies being targeted more severely. Hypothesis 2 is developed below.

H2: Companies listed in developed countries are more negatively affected by phishing announcements

According to APWG, phishing usually targets firms in financial and banking industries because these industries are the most lucrative. In January 2008, the most frequently targeted industry sectors for phishing were financial services (92.4%) followed by ISP (1.5%), Government and miscellaneous (2.3%), and retail (1.5%) (APWG 2008). Therefore, customers from the financial services sector should be most concerned about phishing. They are more likely to switch to another company when one fails to deter phishing. Thus, investors may penalize companies in that sector more severely when phishing occurs. Hypothesis 3 is conjectured below.

H3: Financial and banking industries are severely affected by phishing announcements

In this research, we focused on the stock price of listed companies only. Some phishing attacks may directly target holding companies, which are traded directly in the stock market, for instance, HSBC and Citigroup, while some may target subsidiaries, for instance, West Bank and Smith Barney, whose parents companies are listed rather than themselves. We believe phishing targeting holding companies has a more negative impact on firm value when compared with phishing targeting subsidiary companies because investors may judge the performance of all subsidiaries of a holding company as a whole when making investment decisions. The specific hypothesis is shown below.

H4: Phishing announcements relating to holding companies have a more negative impact than those related to subsidiary companies whose parents are listed

As technology progresses, more and more sophisticated phishing attacks occur. In the past, the most rudimentary phishing attack only used plain text emails purportedly coming from the genuine service providers to ask users to reply with their personal information. Now, phishing email is usually accompanied a hyperlink leading to a bogus Web site, which looks seemingly genuine. In some more recent attacks, apart from a bogus Web site, the adversaries also make use of malware such as keyloggers, viruses, and Trojans to enhance the rate of success (Lininger and Vines 2005). When a customer goes to a phishing Web site or receives a phishing email, the malware may be automatically downloaded to the victims' personal computer. The more sophisticated the phishing attack, the higher is the success rate. In view of this, we conjecture hypothesis 5 as below.

H5: The more sophisticated the phishing attack, the more negative the impact on firm value

As discussed above, the negative impact of phishing relies on the perception of investors. This may require investors to have adequate knowledge and awareness of phishing attacks. As time passes, perceptions of people may change with more knowledge about phishing. We believe in the past, when people had little knowledge of phishing, the impact of phishing announcements on firm value was not as high as more recently when many companies, information security organizations, and government bureaus have taken the initiative to educate customers on phishing. With the wide coverage by the press and government, the awareness about phishing for the general public may have increased. Therefore, we have developed H6.

H6: Impact of phishing increases over time

## Research Methodology

In this research, we followed the widely adopted event study methodology and used the methodology of Dos Santos et al. (Dos Santos et al. 1993) as the main framework because that is the first event study in the stream of management information systems and many event studies in the same field have also followed their methodology. However, we have made some adjustments to the methodology by including criteria such as a larger time window for filtering confounding announcements and selection of appropriate trading stocks. Furthermore, in order to enhance the reliability of this research, we also developed a new step to determine the best fit regression model. In this section, a detailed description of the research methodology is provided.

Initially, we gathered phishing announcements which occurred before 2008 from publicly available security alert databases, phishing alert databases, and ordinary news databases. Repositories from organizations, such as Millersmiles, Websense, Antiphishing Working Group Japan (APWG JP), Hong Kong Monetary Authority (HKMA), Malaysia Computer Emergent Response Team (MyCERT), and Factiva were used. Sharing the same database with APWG, Millersmiles is one of the strategic partners of APWG. Its phishing repository was the largest in the world at the time of research and its daily phishing alerts are frequently subscribed by the general public and commercial companies. Apart from screenshots of phishing emails and fraudulent Web sites, most phishing announcements also included a risk level according to the technical sophistication of the attack. However, one limitation of the repository was that it included a lot of US and UK announcements with few related to companies in other countries. In order to expand our scope of analysis, we included other data repositories. Websense is a commercial company specialized in Web filtering software. It publishes phishing announcements with a wider coverage in Europe and Asia. The phishing announcement repositories of Millersmiles and Websense were the main sources of phishing announcements for this research. In order to further expand our data sources, especially data from Asia, we also used other repositories such as those from APWG JP, HKMA, and MyCERT. Apart from this, we also gathered phishing announcements from official Web pages of some companies, which have a section devoted to security or phishing alerts. Besides data collected from various data repositories, we followed the conventional event study methodology to look for other missing phishing announcements from news repository of Factiva. Factiva has a wide coverage of news throughout the world. We used keywords such as "phishing", "spoof/fraudulent emails", "spoof/fraudulent Websites", etc, to exhaustively search all relevant Factiva news that occurred before 2008.

Secondly, we retrieved useful data from phishing announcements by identifying the target companies as well as specific event dates. All companies, which were not listed or whose parents were not listed at the time phishing occurred or did not have at least 200-trading day data one month prior to phishing announcements, were removed.

Next, for those listed companies, which were too thinly traded, for instance, those listed in PINK and OTC, were all removed because thinly traded stocks may influence the parametric test of subsequent analysis (Chatterjee et al. 2002). Then we filtered announcements, which may confound with other important events such as merger and acquisition, hiring/leaving of senior management, declaration of dividends, and earning announcements. We adopted a 5 day window (2 days before the event, event day, and 2 days after the event) to filter out announcements with confounding events. Next, we retrieved daily trading data for the companies from the day it started to trade to the date of the event from Reuters. However, some companies were delisted at the time of the research and thus we were unable to retrieve the data and those announcements were deleted. Table 2 shows the sample size of all announcements retrieved before and after filtering.

**Table 2. Sample Data**

| Source | Before Filtering | After Filtering |
|---|---|---|
| Millersmiles | 7407 | 2668 |
| Websense | 582 | 181 |
| APWG JP | 32 | 17 |
| HKMA | 113 | 34 |
| MyCERT | 24 | 9 |
| Factiva | 1207 | 78 |
| Others | 30 | 7 |
| Total | 9395 | 2994 |

We categorized tickers of companies according to their listed stock exchanges. Then for each stock exchange, we retrieved major general market composite indices and market composite indices for banking and financial industries because the majority of the sample was from the two industries. Then we followed the conventional methodology to run a regression for each company ticker and its associated market composite indices using 200 historical trading data one month before the phishing announcement date as shown in Table 3 and Figure 1.

**Table 3. Market Indices of Different Stock Exchanges**

| Origin of Stock Exchange | Market Indices | Sample Size |
|---|---|---|
| Australia | S&P/ASX 300 Banks, S&P/ASX 300 Diversified Financials, S&P/ASX Financials, and ASX All Ordinaries Index | 75 |
| Austria | ATX Austrian Traded Index | 1 |
| Belgium | BEL 20 Index, BEL General Financial Financial Index, and BEL Banks Financial Index | 1 |
| Brazil | Sao Paulo SE Bovespa Index | 2 |
| Canada | Toronto SE 300 Composite Index and S&P/TSE Canadian Financials Sector Index | 50 |
| Colombia | Colombia SE General Index | 1 |
| Cyprus | Cyprus Stock Exchange / FTSE Top 20 Index, Main Market Index, CSE General Index, and Banks Index | 1 |
| France | CAC Banks Financial Index, CAC Financials Financial Index, and CAC 40 Index | 25 |

| | | |
|---|---|---|
| Germany | PRIME Xetra Bank Index, PRIME Xetra Financial Sevices Index, HDAX Index, DAX Index | 4 |
| Greece | Athens Stock Exchange FTSE Financial Services Index, Athens Stock Exchange FTSE Banks Index, ASE Main General Index | 3 |
| Hong Kong | Hang Seng Finance Index and Hang Seng Index | 28 |
| India | Bombay SE Sensitive Index and Bombay SE 100 Index | 7 |
| Ireland | ISEQ Overall Index and ISEQ Financial Index | 8 |
| Italy | MIBTEL General Index, Milan SE Bank Historical Index, and Milan SE Financial Services Historical Index | 7 |
| Japan | Nikkei 225 Index, Topix 100 Market Index, Topix 500 Market Index, and TOPIX Stock Price Index | 20 |
| Kuwait | Gih Gcc Ilsmc Index | 2 |
| Malaysia | KLSE Financial Index and KLSE Composite Index | 17 |
| Mexico | INMEX Index and IPC Index | 3 |
| Netherlands | Amsterdam Exchanges Index, AEX Banks Index, and AEX Financial Index | 15 |
| Philippines | Philippine SE Composite Index and Philippine SE Financial Index | 2 |
| Qatar | Doha Securities Market General Index | 1 |
| Romania | Bucharest SE Composite Index and Bucharest SE BET Index | 2 |
| Singapore | Straits Times Index | 9 |
| South Africa | Johannesburg Stock Exchange All Share Industrials Index and Financials Index | 2 |
| South Korea | Korea SE Kospi 200 Index and Korea SE KOSPI Finance Index | 1 |
| Spain | IBEX 35 Index | 28 |
| Sweden | Stockholm Options Marknad OMX Value Index and SWX SP Banks Total Return Index | 2 |
| Switzerland | Swiss Market Index | 4 |
| Taiwan | Taiwan SE Weighted Index and Taiwan SE Banking & Insurance Index | 1 |
| Turkey | Istanbul SE Ulusal 100 Index | 1 |
| United Arab Emirates | National Bank of Abu Dhabi Emirates Stock Market Index, Banking Index, National Bank of Abu Dhabi Banking Sector Index, National Bank of Abu Dhabi Banking Index, and ABN Amro Dubai Total Return Index | 4 |
| United Kingdom | FTSE 100 Index and FTSE All Share Banks Index | 548 |
| United States | AMEX Composite Index, AMEX Financial Index, S&P 500, S&P Banks Industry Group Index, S&P Diversified Banks Index, NASDAQ Financial 100 Index, NASDAQ Bank Index, NASDAQ 100 Index, and NASDAQ Composite Index | 2118 |
| Venezuela | Bursatil Index | 1 |

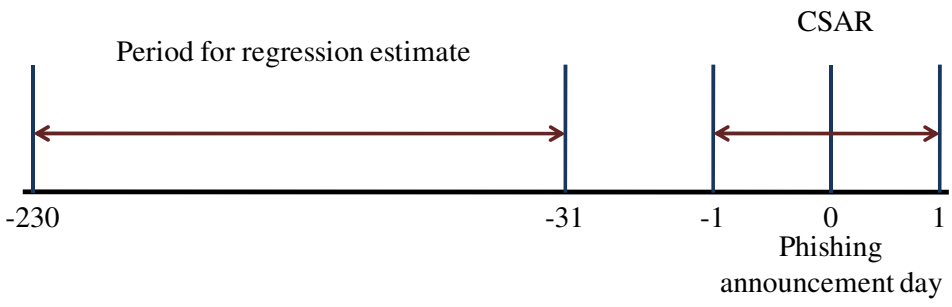


**Figure 1. Time Frame of Event Study**

In order to yield a more robust regression result, for a stock exchange with more than one composite index, we selected the composite index, which gave a higher R square in regression. This is a new step, which was not implemented in prior event study researches, but we believe this step can enhance the robustness and reliability of the research study because a regression model with a higher R square gives a better prediction and thus a more accurate result in computing the abnormal returns in subsequent steps.

Fourthly, we followed the conventional steps of event study methodology to compute the abnormal returns of stock price of each ticker using capital pricing model, $AR_{it} = R_{it} - (\alpha + \beta_t R_{mt})$ for each event *i* on day *t* for market index *m*. α and β are intercept and slope obtained from the regression model. Then we used $AR_{it}$ to calculate standardized abnormal returns using the formula, $SAR_i = \frac{AR_{it}}{\sqrt{Var(AR_{it})}}$ where $Var(AR_{it}) = s_i^2 \left[ 1 + \frac{1}{200} + \frac{(R_{mt} - R_m)^2}{\sum_{t=-230}^{-31} (R_{mt} - R_m)^2} \right]$ and $s_i^2$ is the residual return variance from the regression capital asset pricing model. Cumulative standardized returns (CSAR) is computed using the formula $\frac{1}{N} \sum_{i=1}^{N} CSAR_i$, where $CSAR_i = \sum_{k=-t}^{s} \frac{SAR_{ik}}{\sqrt{s+t+1}}$. Its statistics significance is computed by $Z = \sqrt{N} CSAR$.

## Research Results

The overall impact of phishing announcement is as shown in Table 4. It is shown that phishing announcements had a negative impact on firm value with a loss of 5.1% in CSAR significant at 99% confidence level. Considering the impact on firms with different size, where large firms have annual revenue greater than the mean of US$ 9,633 million, we found that with an average loss of 6.1% the impact for large firms was higher than that for small firms with an average loss of 4.5%. Therefore, H1 is strongly supported.

**Table 4. Overall Research Result**

| | *N* | *CSAR* | *Z* |
|---|---|---|---|
| Overall | 2994 | -5.1% | -2.79** |
| Large firms | 1067 | -6.1% | -1.99* |

| | | | |
|---|---|---|---|
| Small firms | 1918 | -4.5% | -1.96* |

** Significant at 99% confidence level
* Significant at 95% confidence level

When we took origin of companies into consideration, developed countries showed a negative CSAR at -5.3% at 99% confidence level whereas the CSAR for developing countries were non-significant as shown in Table 5. Therefore, H2 is strongly supported.

**Table 5. Research Result by Development Status**

| Type | Countries/Regions | *N* | *CSAR* | *Z* |
|---|---|---|---|---|
| Developed Countries | Australia, Austria, Belgium, Canada, Cyprus, France, Germany, Greece, Hong Kong, Ireland, Italy, Japan, Netherlands, Singapore, South Korea, Spain, Sweden, Switzerland, Taiwan, United Kingdom, and United States | 2946 | -5.3% | -2.89** |
| Developing Countries | Brazil, China, Colombia, India, Kuwait, Malaysia, Mexico, Philippines, Qatar, Romania, South Africa, Turkey, United Arab Emirates, and Venezuela | 48 | 8.0% | 0.55 |

** Significant at 99% confidence level

With regard to industries, we grouped various phishing announcements according to Global Industry Classification Standard (GICS) as defined by Reuters. As some GICS are similar in nature, we further clustered them into 5 different industries, namely, banking, finance, insurance, IT & Telecom, and Others. As shown in Table 6, industries such as finance and IT & Telecom showed the most negative impact, at 99% confidence level. However, contrary to our initial anticipation, the banking industry did not pose a highly significantly negative impact. Therefore H3 is only partially supported.

**Table 6. Research Result by Industries**

| Industries | GICS | *N* | *CSAR* | *Z* |
|---|---|---|---|---|
| Banking | Asset Management & Custody Banks, Diversified Banks, Investment Banking & Brokerage, and Regional Banks | 1443 | -2.6% | -1.00 |
| Finance | Consumer Finance, Diversified Capital Markets, Other Diversified Financial Services, Specialized Finance, and Thrifts and Mortgage Finance | 448 | -10.6% | -2.25** |
| Insurance | Life & Health Insurance, Multi-line Insurance, and Property & Casualty Insurance | 145 | 3.8% | 0.46 |
| IT & Telecom | Application Software, Communications Equipment, Data Processing & Outsourced Services, Integrated Telecommunication Services, Internet Software & Services, Systems Software, Wireless Telecommunication Services | 839 | -8.3% | -2.39** |
| Others | Broadcasting & Cable TV, Casinos & Gaming, Food Retail, Human Resource & Employment Services, Hypermarkets and Supercenters, Internet Retail, Movies & Entertainment, Publishing, and Railroads | 119 | -3.1% | -0.34 |

** Significant at 99% confidence level

With regard to the analysis of target companies of phishing with different types of ownership, the impact of holding companies was significantly negative whereas that of subsidiaries was not. Therefore, H4 is supported. The detail is as shown in Table 7.

**Table 7. Research Result by Company Ownership**

| | *N* | *CSAR* | *Z* |
|---|---|---|---|
| Overall | 2994 | -5.1% | -2.79** |
| Holding Companies | 1306 | -7.3% | -2.65** |
| Subsidiaries | 1688 | -3.4% | -1.39 |

** Significant at 99% confidence level

Considering various methods of phishing attacks, we analyzed only those data retrieved from the repository of Millersmiles because it classified each phishing announcement into 6 risk levels according to their technical sophistication. Table 8 shows the definition of each risk level.

**Table 8. Risk Levels of Phishing Announcements**

| Risk Level | Definition |
|---|---|
| N/A | No risk assessment has been done |
| Low | Little chance to fool others or none of the hyperlinks provided by the phishing scams are valid |
| Low-Medium | Little chance to fool others because of poor features such as broken hyperlinks or invalid URL |
| Medium | Well constructed phishing scam despite bad grammar and spelling |
| Medium-High | Professionally made phishing scam with possibly more dangerous features |
| High | Phishing scam accompanied with virus or other new and rare techniques |

The impact of phishing announcement based on technical sophistication is shown in Table 9. As the sample size of low and low-medium was small, we grouped them into a new category called "< Medium". Among all risk factors, phishing with medium risk showed the most significant result. However, the CSAR associated with high risks was not significant at all. Therefore, H5 does not hold.

**Table 9. Research Result by Risk Factors**

| Risk | *N* | *CSAR* | *Z* |
|---|---|---|---|
| < Medium | 29 | -6.8% | -0.36 |
| Medium | 2260 | -4.8% | -2.29 ** |
| Medium-High | 221 | -3.3% | -0.48 |

| | | | |
|---|---|---|---|
| High | 69 | -5.1% | -0.42 |

** Significant at 99% confidence level

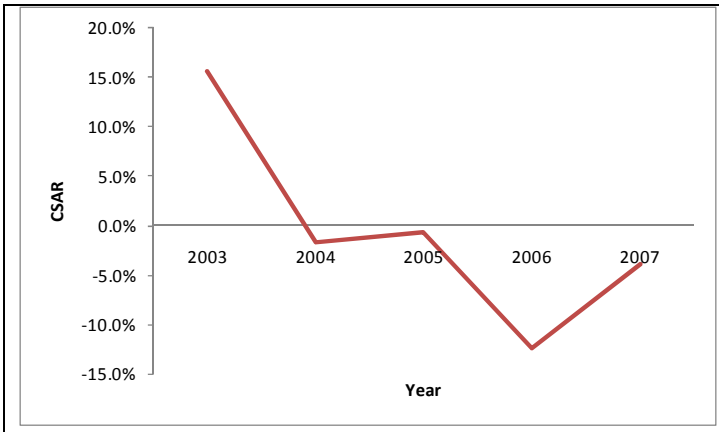


**Figure 2. Change of CSAR over Time**

**Table 10. Research Result by Risk Factors**

| Year | *N* | *CSAR* | *Z* |
|---|---|---|---|
| 2003 | 53 | 15.7% | 1.14 |
| 2004 | 359 | -1.7% | -0.33 |
| 2005 | 745 | -0.7% | -0.20 |
| 2006 | 921 | -12.4% | -3.78 ** |
| 2007 | 916 | -3.8% | -1.16 |

** Significant at 99% confidence level

As shown in Figure 2, a downward trend is indicated when we compared CSAR over the year of announcements. In the very beginning, a phishing announcement did not pose a negative impact to firm value at all. This may indirectly reflect that people in general did not have adequate knowledge about phishing. However, from 2004 onwards, the negative impact was aggravated and in 2006, the CSAR became the most negative and reached the bottom. As shown in Table 10, the CSAR in 2006 was significant at a 99% confidence level. This shows that people are more concerned about phishing and perceive phishing announcements to be a reflection of the weakness of the company. However, in 2007, the CSAR bounced back and became less negative. This may be due to change in perception of investors. The influx of phishing announcements may give investors an impression that phishing is a random attack and may not necessarily be related to the weakness of the company. Therefore, a bounce-back occurred. Hypothesis H6 is not supported.

## Discussion

Some interesting phenomena were discovered in this research. First and foremost, our research gave strong evidence to show that phishing announcements drive down the market value of companies providing e-commerce services. Such a phenomenon exists in both large and small companies although the impact on holding companies was more significant than subsidiaries. It is also shown that the market in general favors companies with adequate information

security measures to protect their customers, and penalizes those firms that do not do so. This gives a strong signal to industrial practitioners to better equip themselves to deter phishing.

Secondly, our findings showed that the impact of phishing was more significant in developed countries when compared with other parts of the world. This might be associated with varied knowledge or exposure to phishing of general public in different countries. As the impact of phishing announcements was highly dependent on the knowledge of investors towards the identity theft, it might be due to this reason the announcements related to developing countries did not yield a significant result.

Thirdly, it was found that the most targeted industries of phishing, such as banking and finance, were not necessarily the most severely affected by phishing announcements. From our research analysis, among the two industries, only companies from the financial industry had the most significantly negative impact although companies from the banking industries also showed a relatively high negative return. The frequent appearance of phishing announcements from the banking industries might dilute the perception that being attacked by phishing is equivalent to poor performance in information security. As a result, the banking industry had a lower impact than the finance industry. Nevertheless, apart from the finance industry, IT and Telecom was another significantly affected industry. The high impact might be due to higher expectation of people in general that companies from the IT and Telecom industry should have better expertise and technologies to deter phishing. Therefore, when they were targeted by phishing, investors perceived that such companies were inferior to their peers and thus penalized them more severely.

Furthermore, our research results suggested that people in general did not penalize phishing attacks with higher technical sophistication. This again might be related to the knowledge of investors to phishing. People in general might treat all types of phishing attacks equally and thus announcements associated with high risks did not show the most significantly negative impact.

Finally, our research indicated a change in perception of phishing over time. As shown in Figure 2, the CSAR showed a downward trend from 2003 to 2006. This corresponded to the increasing number of phishing incidents throughout the period. As shown by APWG, the year to year rates of reported phishing incidents were 2.7%, 56.0%, and 8.0% from 2004-2005, 2005-2006, and 2006-2007 respectively (APWG 2005; APWG 2006; APWG 2008). From 2005-2006, a sharp increase was observed. With the surge in phishing attacks and wider coverage by the press, people understood the phenomenon of phishing more and thus had a stronger perception that being attacked by phishing is associated with poor corporate information security. However, in 2007, a decrease in the impact of phishing was observed. This again might be related to changes in perception. As more and more phishing incidents occurred, people might have become de-sensitized about such news and thus did not penalize companies for being the target of phishing so seriously. In order to justify such a change of perception, we need more time and data to implement a longitudinal study. Such an analysis could be the subject of future research.

## Conclusion

This is a pioneering event study in the area of phishing. We have successfully shown that there exists an indirect link between phishing announcements and firm value. We made a significant improvement when compared with other similar studies in the area of information security using the event study methodology in terms of sample size and selection of the best fit regression model. By careful analysis of phishing announcements, we discovered that phishing had a significantly negative impact on firm value regardless of firm size. However, the origin of phishing might differ from one place to another. The impact on companies listed in developed countries was more negative than those listed in developing countries. This might be related to the frequent occurrence of phishing incidents and also the richer knowledge of investors towards phishing. However, if the target company was a holding corporation, the impact was more severe and statistically significant when compared with the subsidiaries. Also, our results seemed to suggest that the technical skills of phishing did not have much of a relationship with the impacts of phishing. However, time factors might influence the results. This might be related to the change in the perception of people towards phishing announcements over time. At the very beginning, the impact of phishing announcements was very little due to the inadequate exposure or knowledge about phishing. But the impact became more and more negative with the passage of time and in 2006, the highest negative impact was observed. However, it became less strong in 2007. The mitigation of the effect might be related to influx of too much phishing information and people becoming less inclined to penalize firms which failed to deter phishing. Nevertheless, as one of the future research areas, we will collect more data to conduct a longitudinal study to analyze the change in investors' perception to

phishing over time. By quantifying the indirect financial loss of phishing, we hope that our research can urge industrial practitioners to pay more attention to the negative impacts of phishing attacks and adopt more adequate anti-phishing measures to safeguard their customers and deter phishing. Furthermore, we believe that our research can contribute to academia by bridging the research gap in both phishing research and event studies.

## Acknowledgements

We thank Thomson Reuters for their help in retrieving some delisted stock data for this paper.

## References

Acquisti, A., Friedman, A., and Telang, R. "Is there a cost to privacy breaches? An event study," Proceedings of Twenty-Seventh International Conference on Information Systems, Milwaukee, 2006, pp. 1563-1580.

APWG "Phishing activity trends report December 2005," Anti-Phishing Working Group, 2005, pp. 1-15 (http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf).

APWG "Phishing activity trends report December 2006," Anti-Phishing Working Group, 2006, pp. 1-15 (http://antiphishing.org/reports/apwg_report_Dec2006_FINAL.pdf).

APWG "Phishing activity trends report: Report for the month of January, 2008," Anti-Phishing Working Group, 2008, pp. 1-9 (http://www.apwg.org/reports/apwg_report_jan_2008.pdf).

Bohme, R., and Holz, T. "The effect of stock spam on financial markets," Proceedings of the Fifth Workshop on the Economics of Information Security, Cambridge, 2006, pp. 1-24.

Bose, I., and Leung, A.C.M. "Unveiling the mask of phishing: Threats, preventive measures, and responsibilities," Communications of the Association for Information Systems (19:24) 2007, pp. 544-566.

Brandt, A. "Phishing anxiety may make you miss messages," PC World (23:10) 2005, p 34.

Campbell, K., Gordon, L.A., Loeb, M.P., and Zhou, L. "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," Journal of Computer Security (11:3) 2003, pp. 431-448.

Cardline "Phishing could hurt e-commerce, study finds," Cardline (http://www.accessmylibrary.com/coms2/summary_0286-21323317_ITM).

Cavusoglu, H., Mishra, B., and Raghunathan, S. "The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers," International Journal of Electronic Commerce (9:1) 2004, pp. 69-104.

Chatterjee, D., Pacini, C., and Sambamurthy, V. "The shareholder-wealth and trading-volume effects of information-technology infrastructure investments," Journal of Management Information Systems (19:2) 2002, pp. 7-42.

Choo, K., Smith, R., and McCusker, R. "Future directions in technology-enabled crime: 2007-09," Australian Institute of Criminology, 2007.

Dhamija, R., and Tygar, J.D. "The battle against phishing: Dynamic Security Skins," Proceedings of the 2005 Symposium on Usable Privacy and Security, ACM Press, Pittsburgh, Pennsylvania, 2005, pp. 77-88

Dos Santos, B.L., Peffers, K., and Mauer, D.C. "The impact of information technology investment announcements on the market value of the firm," Information Systems Research (4:1) 1993, pp. 1-24.

Geer, D. "Security technologies go phishing," IEEE Computer (38:6) 2005, pp. 18-21.

Goth, G. "Phishing attacks rising, but dollar losses down," IEEE Security & Privacy Magazine (3:1) 2005, p 8.

Herzberg, A., and Gbara, A. "TrustBar: Protecting (even Naïve) Web users from spoofing and phishing attacks," 2004.

Hovav, A., and D'Arcy, J. "The impact of denial-of-service attack announcements on the market value of firms," Risk Management and Insurance Review (6:2) 2003, pp. 97-121.

Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F. "Social phishing," Communications of the ACM (50:10) 2006, pp. 1-10.

Jakobsson, M. "Distributed phishing attacks," Proceedings of DIMACS Workshop on Theft in E-Commerce, New Jersey, 2005, pp. 1-10.

James, L. Phishing exposed Syngress, Rockland, Mass., 2005.

Kannan, K., Rees, J., and Sridhar, S. "Market reactions to information security breach announcements: An empirical analysis," International Journal of Electronic Commerce (12:1) 2007, pp. 69-91.

Kirda, E., and Kruegel, C. "Protecting users against phishing attacks with AntiPhish," Proceedings of the Twenty-ninth Annual International Conference on Computer Software and Applications, 2005, pp. 517-524 Vol. 512.

Libbenga, J. "German Postbank uses e-signatures to curb phishing," The Registrar (http://www.theregister.co.uk/2006/04/07/postbank_curbs_phishing/).

Lininger, R., and Vines, R.D. Phishing: cutting the identity theft line Wiley, Indianapolis, Ind., 2005.

M2 Presswire "One in five users affected by daily phishing onslaught, reveals Sophos," in: M2 Presswire, 2006.

Nowell, P. "Bank of America rolls out new online security system," USA Today (http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-07-13-bank-security_x.htm).

Telang, R., and Wattal, S. "An empirical analysis of the impact of software vulnerability announcements on firm stock price," IEEE Transactions on Software Engineering (33:8) 2007, pp. 544-557.

Wu, M., Miller, R.C., and Little, G. "Web wallet: Preventing phishing attacks by revealing user intentions," Proceedings of the Second Symposium on Usable Privacy and Security, ACM Press, Pittsburgh, Pennsylvania, 2006, pp. 102-113.