Impact Analysis of Phishing Announcements on Market Value of Hong Kong Banks

Alvin C. M. Leung and Indranil Bose

***Abstract*—In this research, we adopted event study methodology to analyze the impacts of 25 phishing announcements released by the Hong Kong Monetary Authority from 2003 to 2007 on market value of 10 local banks. The results showed that negative market return occurred immediately after the phishing incidences were announced. The intensity of the negative impacts became more severe as time passed. For banks being targets of repeated phishing attacks, the most recent attack brought more negative market return than initial attack. Our research also showed that apart from direct financial loss, phishing also attributed to indirect financial loss to market value of e-commerce enabled banks. Better preparation to deter phishing is necessary to reduce the potential financial loss.**

***Index Terms*—Event study methodology, Hong Kong banks, market value, phishing, phishing announcements.**

I. Introduction

E-commerce is one of the fastest growing industries nowadays. By 2009, the revenue generated from online business-to-customer market is expected to reach US$213 billion [5]. Making use of social engineering skill and technical subterfuge, phishing, an online identity threat, poses a hindrance towards the development of e-commerce. Not only does it cause financial loss to victims as a result of identity theft, phishing also undermines confidence of customers towards e-commerce service offered by the companies. The average per victim financial loss as a result of phishing emails in 2006 was US$1,244 [2]. Nevertheless, the loss as a result of customers switch to other companies or even abandon the e-commerce service had yet considered. We believe that the total financial loss would be even higher when indirect costs had been taken into account.

In this research, we tried to estimate the indirect cost of phishing from the perspective of market value, which is measured by the return from stock. The change of return of stock may indicate the perception of investors towards the prosperity of the company. Following the event study methodology, we isolated other confounding and solely investigated the influence of phishing announcements on market value. We hope that this research can enhance the understanding of the indirect impact of phishing on e-commerce companies.

II. Literature Review

Research on phishing can be categorized into two groups: technical research and phenomenal study. For technical research, most researchers focus on the development of new anti-phishing tools to combat phishing attacks. Recent research products include Dynamic Security Skin [3], Web Wallet [14], TrustBar [6], and AntiPhish [11]. Though many innovative anti-phishing products exists, not many of them are adopted by e-commerce companies and it was observed that some banks were not well prepared against or even unaware to phishing at all [12].

Another stream of phishing research focuses on phenomenal study. Social engineering skills, lack of knowledge, visual deception, and lack of attention [3, 9] were found to be critical factors of success of phishing attacks. Nevertheless the analysis of indirect financial loss is scarce in phishing literature. This research may help to fill in the research gap. We hope to raise the awareness of e-commerce companies to understand the seriousness of phishing so as to adopt better anti-phishing measures to deter the crime and minimize the potential indirect loss due to the threat.

To study the indirect impact due to sudden events, in the field of Management of Information Systems (MIS), there are quite a number of researches utilizing the event study methodology to analyze the change of market value of companies due to the sudden events. Dos Santos et al. first used the methodology to analyze impact of IT investment to firm value in the field of MIS [4]. The study was later

Indranil Bose is Associate Professor of School of Business, University of Hong Kong (corresponding email: bose@business.hku.hk).

Alvin C. M. Leung is an MPhil student of School of Business, University of Hong Kong (corresponding e-mail: alvinleung@business.hku.hk).

refined by Im et al [8]. Same research methodology was also applied to e-commerce announcements [13] and denial-of-service attacks [7]. Our research used the same methodology adopted by Dos Santos et al. but applied it in a different context to analyze the impact of phishing announcements on firm value.

III. Research Questions

In this research, we would like to answer two main research questions: (1) How do phishing announcements in general affect market value of firms? As the success of phishing incidences may somehow imply the ineffective preparation of companies against the crime, we conjectured that phishing announcements negatively influence the market value of e-commerce companies. (2) How does market value of firms change with repeated phishing announcements? When a firm suffers from repeated attacks, investors may perceive such attacks as inevitable threat. Thus we conjectured that the initial attack show the most negative influence to market value.

IV. Research Methodology

We followed the event study methodology as illustrated in the work of Dos Santos et al. [4]. Firstly, we gathered announcements related to phishing attacks from the official Web site of Hong Kong Monetary Authority. 109 phishing related announcements from May 20, 2003 to November, 2007 were obtained. Then we filtered the announcements to those related to Hong Kong banks alone and there were about 68 records. Next we excluded those non-listed companies at the time of phishing attacks and filtered out those with other confounding events such as earning, merger, and acquisition three days before and after the phishing announcements. 25 phishing announcements of 10 local banks were retained for further analysis.

Secondly we retrieved stock data of the 10 firms 202 days before and 3 days after the occurrence of the event and the corresponding Hang Seng Index, which is the market index in Hong Kong, in the same period. Using the capital asset pricing model, we then estimated the returns of each stock by the formula $R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$, where R_{it} is the return of stock i on day t, $R_{it} = \dfrac{Stock_{it} - Stock_{it-1}}{Stock_{it-1}}$, R_{mt} is the return of market (i.e. Hang Seng Index) on day t, α_i and β_i are company dependent coefficients to be determined and is the random error of firm i on day t. We used 200 trading data, which were at least one day before the announcement of phishing as shown in Figure 1 to build a regression model so as to estimate α_i and β_i. The reason of doing so is to get as many sample data, which is closed to the event, as possible. As the report date of event is usually one day after the actual occurrence of the event, investors may have already learnt about the event before the date of report. Therefore, our estimation period is at least one day before the announcement day of phishing.

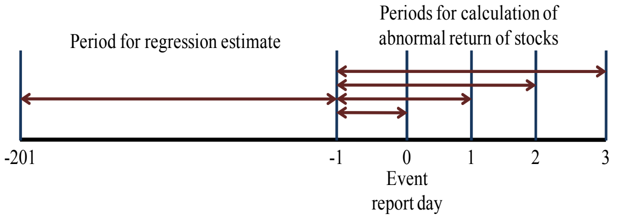
Period for regression estimate
Periods for calculation of abnormal return of stocks
-201
-1
0
1
2
3
Event report day

Figure 1. Periods for Data Analysis

Thirdly, we used the capital asset pricing model to compute the standardized abnormal return of stock i on day t using the formula $AR_{it} = R_{it} - (\alpha + \beta_t R_{mt})$. Then we computed the standardized abnormal return to stock i on day t by $SAR_i = \dfrac{AR_{it}}{\sqrt{Var(AR_{it})}}$ where

$$Var(AR_{it}) = s_i^{\,2}\left[1 + \frac{1}{D} + \frac{(R_{mt} - R_m)^2}{\sum_{t=-201}^{-2}\left(R_{mt} - R_m\right)^2}\right]$$

and s_i^2 is the residual return variance from the regression capital asset pricing model.

Fourthly, we computed the cumulative standardized abnormal return of stock i over a period of time [-t, s] where t is the number of days before event day and s is the number of days after the event day using the formula $CSAR_i = \sum_{k=-t}^{s} \dfrac{SAR_{ik}}{\sqrt{s+t+1}}$. For a sample of N stocks, the cumulative standardized abnormal return is $\dfrac{1}{N}\sum_{i=1}^{N} CSAR_i$ and the corresponding statistical significance is computed by $Z = \sqrt{N}CSAR$. The periods of estimation that we used were [-1, 0], [-1, 1], [-1, 2], and [-1, 3]. We first analyzed the entire sample of 25 phishing announcement. Then we investigated phishing announcements of each of 10 banks. There were 7 banks with more than 1 phishing announcements. We later analyzed the change of the effects of the announcements over time.

V. Research Results

Table 1 below shows the result of 25 phishing announcements on 10 Hong Kong banks as a whole. The positive sign of CSAR indicates that the stock exceeds the prediction and vice versa while the absolute value of CSAR indicates the magnitude, which exceeds the expectation. As shown in the table, investors tended to penalize firms negatively, which were subject to phishing attacks though the Z-value indicates that the result was not statistically significant with p value of about 49% to reject the null hypothesis of zero change. As time progresses, the magnitude of CSAR and the corresponding Z-value increase. On the third day after phishing announcements were released, the CSAR and Z-value reach the maximum in magnitude.

Table 1. Overall effects of phishing announcements on HK banks

	[-1, 0]	[-1, 1]	[-1, 2]	[-1,3]
CSAR	-0.0023	-0.0032	-0.0048	-0.0054
Z-Value	-0.0114	-0.0158	-0.0242	-0.0270

Table 2 shows all 10 banks under investigation. Banks suffering repeated phishing attacks were shown with the attack showing the maximum magnitude of $CSAR_i$. Apparently, the strength of $CSAR_i$ varied from bank to bank. Some indicate that the initial phishing attack was the most serious while others indicate that the last phishing attack was the most severe.

Table 2. Banks with repeated phishing attacks showing maximum magnitude of $CSAR_i$

		Attack with maximum magnitude of $CSAR_i$			
ID	# of Attacks	[-1, 0]	[-1, 1]	[-1, 2]	[-1, 3]
1	1				
2	2	1st	1st	1st	2nd
3	2	2nd	2nd	2nd	2nd
4	1				
5	5	5th	5th	5th	5th
6	1				
7	4	4th	4th	4th	4th
8	3	1st	1st	1st	1st
9	3	1st	3rd	1st	1st
10	3	1st	3rd	3rd	3rd

However, when we take into consideration of the CSAR of first phishing announcement of banks suffering repeated attacks as shown in Table 3, the magnitudes of CSAR over the 4 assessment periods were very small, which were close to 0 and the signs of some of the assessment periods were even positive. It shows that the investors did not react vigorously to the initial attack and the return of stock was almost the same as predicted by the regression model.

Table 3. Result of initial phishing announcements for banks with repeated attacks

	[-1, 0]	[-1, 1]	[-1, 2]	[-1, 3]
CSAR	0.0009	0.0022	0.0002	-0.0023
Z-Value	0.0023	0.0059	0.0006	-0.0061

Nevertheless, taking into consideration of the latest phishing attack, we found that investors generally reacted more vigorously. The magnitude of CSAR reached a maximum 3 days after the attack while the corresponding Z value is the most negative as shown in Table 4. The research results show the change of attitude of investors towards phishing announcements. Phishing announcements were perceived more negatively than before.

Table 4. Result of latest phishing announcements for banks with repeated attacks

	[-1, 0]	[-1, 1]	[-1, 2]	[-1, 3]
CSAR	0.0005	0.0016	-0.0025	-0.0052
Z-Value	0.0013	0.0040	-0.0060	-0.0126

VI. Findings and Discussion

As shown in Table 1, investors in general penalize banks, which were subject to phishing attacks, negatively. As a result of phishing, customers of the firms may lose confidence towards e-commerce service offered by the banks and may switch to other companies or even minimize or abandon the online transaction. In the view of potential loss of customers, investors may be pessimistic towards the future revenue generated by the company. Thus they may short sell the stocks upon hearing the news. Therefore, a negative sign of CSAR was shown over the 4 assessment periods. Due to imperfect dissemination of information, the most negative response was not resulted immediately after the news was released. As time progressed, it was shown that the CSAR became more and more negative and the corresponding Z-value became the greatest 3 days after the announcement of phishing was disclosed.

With regard to repeated phishing attacks, investors reacted more negatively in recent attacks when compared with the initial ones. This may indicate that investors' awareness of phishing has been heightened in recent years. Therefore, they tended to penalize those firms, which were unable to deter phishing, more severely than before. This gives a signal to e-commerce firms to be better prepared against phishing so as to prevent any potential loss in market value.

VII. Future Research Areas

In this research, our sample size is small because we only based on the announcements in Hong Kong alone. A larger sample would definitely help enhance the statistic significance and representativeness of the findings. As a future research, we would like to enlarge the sample size by including other phishing announcements from countries, which are frequent target of phishing, such as US.

Also, more variety of e-commerce companies, apart from those from the banking industries, may be included to in the research. Though banking is one of the frequent targets of phishing, online bidding companies, electronic auction companies, and other retailing firms are also influenced adversely by phishing. Analyzing companies with diverse background may better understand the indirect impact of phishing on market value.

On the other hand, we would like to analyze the impact of phishing announcements based on various types of phishing attacks, which can be classified according to its phases of life cycle, namely, preparation, mass broadcast, mature, and account hijack [1] or various phishing techniques involved, for instance, deceptive, malware-based, DNS-based, content-injection, man-in-the-middle, and search engine [10]. Impacts of different types of phishing attacks may vary from one category to another. Analyzing those effects, we could establish better understanding over the impact of phishing on market value of firms.

VIII. Conclusion

E-commerce has long been plagued by phishing. Apart from direct financial loss to victims of phishing attacks, our research also reveals the indirect loss of market value of e-commerce companies. Though our sample size is small and thus our research results are not statistically significant at a reasonably low confidence level, our research results still reveal that Hong Kong banks may suffer from negative return of stock due to inability to deter phishing attacks.

Also, as information dissemination is not perfect, our research result shows a growing magnitude in terms of cumulative standardized abnormal return (CSAR). The CSAR is the most negative on the third day after the phishing announcement is released.

Furthermore, investors are becoming more and more concerned about the preparedness of firms against phishing. The impacts of recent phishing announcements were more negative than those of the initial attack announcements for firms suffering from repeated attacks. This gives a warning signal to firms, which have yet prepared against phishing at all.

In the future, we are planning to enlarge the sample size by including more phishing announcements from other countries and from other industries other than banks. We would also like to analyze the impact of announcements of different types of phishing attacks on firm value. We hope that our research could enrich the understanding of the impact of phishing to the e-commerce industry.

References

[1] I. Bose and A. C. M. Leung, "Unveiling the mask of phishing: Threats, preventive measures, and responsibilities," *Communications of the Association for Information Systems,* vol. 19, pp. 544-566, 2007.

[2] S. Carter, "Scam artists are phishing for your information," in *Warricknews*, 2007. Available: http://www.tristate-media.com/articles/2007/05/02/warricknews/editorial/01carter.txt

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

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

[5] GSI Commerce, "GSI E-Commerce Solutions, Reports Net Revenue Growth," GSI Commerce 2007.

[6] A. Herzberg and A. Gbara, "TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks," 2004.

[7] A. Hovav and J. D'Arcy, "The impact of Denial-of-Service attack announcements on the market value of firms," *Risk Management and Insurance Review,* vol. 6, p. 97, 2003.

[8] K. S. Im, K. E. Dow, and V. Grover, "Research report: A reexamination of IT investment and the market value of the firm - An event study methodology," *Information Systems Research,* vol. 12, p. 103, 2001.

[9] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM,* vol. forthcoming, pp. 1-10, 2006.

[10] M. Jakobsson and S. Myers, *Phishing and countermeasures : understanding the increasing problem of electronic identity theft*. Hoboken, N.J.: Wiley-Interscience, 2007.

[11] E. Kirda and C. Kruegel, "Protecting users against phishing attacks with AntiPhish," in *Proceedings of the Twenty-ninth Annual International Conference on Computer Software and Applications*, 2005, pp. 517-524 Vol. 2.

[12] A. C. M. Leung and I. Bose, "Assessing Anti-phishing preparedness among Singapore Banks " in *International Multiconference of Engineers and Computer Scientists 2007*, Hong Kong, 2007, pp. 1020-1025.

[13] M. Subramani and E. Walden, "The impact of e-commerce announcements on the market value of firms," *Information Systems Research,* vol. 12, p. 135, 2001.

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