

Strategies for The Security of Online Payments in E-commerce

Chen Zhang, Shijie Jiang, Bin Huang
School of Media Studies&Humanities
Zhejiang University City College
Hangzhou, 317000, China
Email: Zhangchen0007@gmail.com

Abstract—Online payment is apparently the key for the online transactions, so its security issue becomes the center of focus in the e-commerce development. In China, however, the information leakage, transaction fraud and other security issues have occurred so frequently that they have severely affected the customer confidence, and have become one of the major blockages in the e-commerce development. This article intends to have an in depth discussion of online payment security issues, examining current situations and problems in security technology, corporate social responsibility, and also propose appropriate strategic recommendations.

Keywords-E-Commerce, Security Issue, strategy

I. INTRODUCTION

In recent years, the amount of the online transaction in China maintains a stable growth. According to the statistics by iResearch and the latest data from "30th China Internet Development Statistics Report", 2012, second quarter, the overall deal size of Chinese e-commerce market was 1.88 trillion RMB, grew at the rate of 25.0% year-on-year and 7.3% quarter-on-quarter. More than 90 % of the volume of transactions from the online payment, online payment is visibly the mainstream of electronic payment. As a huge contributor to the transaction size and core of e-commerce, online payment allow users to access to banking services in all over the world with conveniently and timely. Until July,2012, China's online payment users grow up to 187 million. The netizen utilization rate up to 34.8%,more than 20 million subscribers growth, the growth rate of 12.3%, netizens utilization rate is increased by 2.3%, compared with 2011.

At present, there are two main basic patterns of online payment, one is bank for Business payments, namely online bank, the other is the third payment platform for business payment , such as 'Alipay'. While with the growth and expansion of online transactions in business, we are also deeply aware of the online payment security issues which is a major bottleneck in e-commerce.

II. ONLINE PAYMENT SECURITY ISSUES

Online payment is not only a kind of payment and settlement behavior based on Internet, but also the important basis of Internet economic activity. However, due to the openness of the network itself, as well as the limitations of the current network technology, online payment faces with various security threats, and they also raise a variety of

security issues in the transaction process, including payment information leakage, transaction fraud, network system risks and so on.

A. The leakage of customer information

Online payment and social network information coexist in the Internet; the Internet activities in all links may lead to a lot of unnecessary losses, because the absence of safekeeping and privacy information, password interception, leakage, risk etc. In addition, some of the transactions must be submitted with the ID card number and the account information. In case the operating personnel leaks the information, then it leads to the customer loss. For example, in April this year, more than 30 credit card holders were swiped for the fraudulent use of funds through the third-party payment platform in China. The whole loss involved 2 million RMB.

B. The trade fraud problems

Transaction fraud which mainly refers to the fact that the identification of both sides of the payment is not enough, providing the chance for dishonest transaction fraud, including "phishing" fraud risk, businesses disappearing after receivables and other fraud behaviors. It becomes apparent that the profit-driven feature of network illegal acts, large electronic business, financial institutions, the third party payment online website a phishing main imitation object,large-scale e-commerce, financial institutions, third-party online payment site are regarded as the imitate object by phishing. RISING Co. Ltd. released related alarm about the new varietal virus in 29th August 2008, for the impactive virus named Net super Trojan came back again since it has been terminated two years ago. Payment security companies experience these troubles repeatedly and are facing a huge challenge to overcome them.

C. The online payment system risk

Due to improper maintenance or technical support for the payment processes information systems, the system can be paralyzed and important user information can be lost because of the error in a transaction. For instance, the problems of the web sever cause the termination and delaying of payment.

III. THE CAUSE ANALYSIS OF ONLINE PAYMENT SECURITY ISSUES

This article is analyzed in sight of man-made cause and natural cause, which are large influence on online payment security factors.

A. The anthropogenic causes

1) *The lack of safety awareness and poor operating habits:* The different degree of fluke mind, covet petty gain, and not carefully identify the authenticity of a web site are the performance of the lack of safe aware. The results can only make the customers be trapped. At the same time, customers' distrust on online payment, concerns about security issues so that the factors of the the online payment development is one of the main factors.

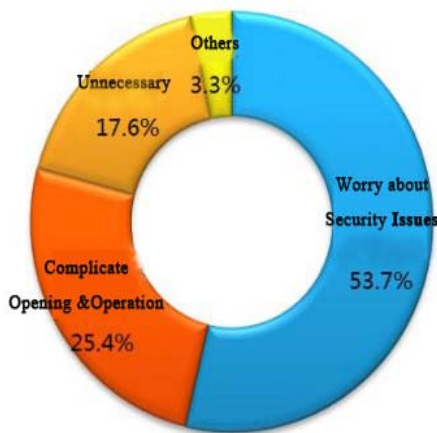


Figure 1. The main reasons for Internet user not using the online payment
Source: Enfodesk

Among the main reasons for Internet users not using online payment, "Worry about security issues" takes up a large proportion of 53.7%, the percentage of the thinking of "Complicated Open and operation, operation" was 25.4%, but the fact is that, at present, according to the in-depth interview done by the main payment company, the ratio of users who have occurred to security issues is less than 5/10000. Online payment with its flexibility and speed to avoid the traditional payment that has the inconvenience from space and time has great advantages: people who are familiar with online payment should know that its operation is simply to acquire. They worry excessively and feel unwilling to accept it, result from being short of the right cognition on the online payment. (please refer to Figure 1)

2) *Consecutive malicious activity, Disrupting the market order:* Online exchange with the great opportunities and great profits don't fail to attract those network invaders who are speculate. As the number of the "online robber" boosts, the black industry is in the constant development and is becoming a complete industrial chain form. As the monitoring data of 360 Security Center, the whole underground Trojan industry professionals already close to millions of scale. If hackers have massive manipulation, they

will not only become a major threat to online payment security, but will also do significantly harm to society.

B. The random causes

1) *Imperfect security protocol:* Security protocol is the hot spot in Online Payment technical security issues. So SSL and SET become the focus. Though SSL applied to a wide range, security is not as good as the latter one which has high cost, complicate operation and difficulty in spreading. In a word, No matter which kind of security protocol used, both are unsatisfactory.

2) *Browser Spy on User Privacy:* The 360Safety Browser, usage rate is less than Internet Explorer. It was discovered that there was spying on user's private information and data was obtained without permission. From a security point of view, a lot of netizen refuse to use this dangerous browser.

3) *What Results in The Derivative Problem is Online Payment Platform Itself:* However Online bank and Third-party payment, as the payment platform, are faced with numerous consumers. Neither can provide personalized service in one-to-one. That is unavoidable issues.

IV. COUNTERMEASURE FOR ONLINE PAYMENT SECURITY ISSUES

A. The Correct guide customers to problem of cognition, culture their confidence

The data and phenomena in the customers' own cause analysis shows, in fact, the overall online payment security environment is much better than that the customer concerns about. The customers who accounted for the two largest proportion of viewpoints are hovering at the edge of the crowd which use the online payment, as long as they try to guide correctly, help them construct a positive understanding of online payment, strengthen the confidence of customers and potential customers of online payment, then laid a good market foundation for the healthy development of the entire online payment.

Primarily, the customer should be "settle the heart", by the way of authoritative opinion and reports through the mass communication, and the primary purpose must be stuck to making the users understand the real pay online. The report content can be offered by a few big online bank and the third party payment platform, e-business enterprise, online payment supervision department. It be carved and disseminated by the mass media, and attract the attention. On the one hand is to guide the user's cognitive direction, the other hand is to realize information symmetry. This has a relatively comprehensive, correct and true understanding and knowledge of the online payment.

The contents are supposed to be related to these detailed suggestions for the customers: to heighten the vigilance, and it is recommended to type the address of the e-commerce websites and don't logged in the unfamiliar site, especially the websites which through the other URLs should be carefully checked of the domain name, then identify the authenticity; don't be credulous of the URLs sent by others; to install anti-virus software and upgrade virus database in time; be careful if the sellers claim that they didn't receive

the transaction amount, then make sure its reality by contacting the customer service immediately, and do not believe the rhetoric which is said by the lawbreakers to pay again, to prevent a further loss; to choose the browser which could identify the authenticity of the website assists you to recognize the phishing website; besides, customers should pull out the U aegis of online bank as soon as they finish the online transaction.

B. Improve laws and regulations,strict the implementation of a system of penalties to keep a norm order

In order to provide online payment with a good legal environment, the government is supposed to speed up formulation and improve relevant online payment measures, making specific provision in term of the legislation purpose, scope, basic principles, definition, type,subject of the online payment, the supervision and management department, the online payment for examination and approval and the authentication etc. The relevant supervisory departments should take actions and tackle the fundamental business credibility problem, thus a real-time monitoring of the accounts of merchant transactions should be provided. Later it was abnormally found, to take immediate processing approach, to take the necessary measures in case of preventing fraud. Strict rules in trade merchants must be signed margin agreement, in order of the merchant fraud.

C. SET and SSL coexistence and complementary advantages

Combined with the specific circumstances of China, it can be predicted, the e-commerce security agreement in China will be the development trend of coexistence of the SET and SSL, and complementary advantages. That is to say, SET protocol between the merchant and the bank, which connect with customers still using the SSL protocol. This scheme does not only avoid installing software on the client-side, but also attains many advantages provided by the SET.

D. The browser company should balance its interests and social responsibility.

Informational search rules can ensure the security of user's information. Moreover, it's so necessary to strengthen the supervision of public opinion for the individuals and mighty the media.

E. Maintain the online payment platform system and risk control

On the one hand, upgrade the system and daily maintenance collaborate to build a more powerful endurance

to withstand and fix loophole in the repairs application system. On the other hand, the online bank and Third-party payment can work with the e-payment solutions providers, such as 'Chinabank payment'.Its measures of the controlling payment security is to provide professional and personalized risk controlling model for the TOP FROU BANKS, CUP merchants,they are by means of the advanced risk controls of risk identification database, the neural network technology, location identification, decision, etc.

F. To strengthen consumer protection by insurance companies

The online payment platform can come up with the type which can match the online payment in order to collaborate with the property insurance companies, like The Taobao return freight insurance. Both the seller and buyer can purchase the insurance in order to ensure their respective interests. Consumers can also purchase the insurance provided by the insurance company, in order to ensure their property.

V. CONCLUSION

Online payment, as a newly developing, convenient, fast and real-time mode, plays an increasingly irreplaceable role in E-commerce. Security issues should be paid more attention. As Visa said, The security of Entire online payment industry isn't measured by the security measures taken; however, it depends on the weakest link. In other words, to improve risk resistance capacity in every weak link is the best way to effectively ensure whole payment industry security.

To summarize, all aspects of online payment, such as security protocols, browsers, users, businesses all should improve, being perfect, jointly guarantee the security of the payment.

REFERENCES

- [1] "2011 China the third-party payment security on Internet research report," Enfodesk,Nov.2011
- [2] "China Online payment comprehensive report of the year 2012," Enfodesk,Jun.2012,p.19
- [3] Q.H. Shuai, Online Payment and Security: Peking University Press, Apr.2010,pp.237-264
- [4] J. Hou,"The SET Protocol Defective Analysis and Improvement Scheme,"New Technology and New Products of China,No.23,2011,p.38