Decision Support Systems 45 (2008) 897–912

Contents lists available at ScienceDirect

Decision Support Systems

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

Assessing anti-phishing preparedness: A study of online banks in Hong Kong

Indranil Bose *, Alvin Chung Man Leung

Room 730 Meng Wah Complex, School of Business, The University of Hong Kong, Pokfulam Road, Hong Kong

ARTICLE INFO

Article history:
Received 4 August 2007
Received in revised form 24 January 2008
Accepted 5 March 2008
Available online 13 March 2008

Keywords:
Accessibility
Anti-phishing
Anti-phishing preparedness
Assessment
Banking industry
Hong Kong
Information content
Usability
Web site analysis

ABSTRACT

Phishing has enormous impacts on the financial industry. This research aims to investigate anti-phishing preparedness of banks in Hong Kong. Web sites of registered Hong Kong banks are analyzed. Information related to phishing and anti-phishing measures adopted by banks are gathered and scores are assigned to banks according to a model measuring accessibility, usability, and information content. A combined score is computed for each bank by measuring the average performance of the bank Web site in all three aspects. The analysis revealed that banks in Hong Kong were generally prepared for countering phishing attacks, and separated out into three clusters that differed in terms of accessibility. The research identified that phishing information was easier to access and was richer in content and coverage compared to information related to anti-phishing measures. Although banks attached importance to information related to anti-phishing measures they needed to improve the accessibility of such information on their Web sites and needed to provide anti-phishing measures related information corresponding to all possible types of phishing attacks including malware and phishing e-mail.

1. Introduction

Phishing is an identity fraud with a short history of 12 years [38] but a tremendous growth rate of 74.0% from September 2006 to September 2007 [4]. It is defined as “a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential and sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion” [37]. It is known that 5% of recipients of phishing e-mails have fallen into the trap [55]. Financial sector is the most popular target of phishing with 91.3% of phishing scams targeted to this industry in September 2007 [4]. The financial loss to the entire business sector has been huge with a direct financial loss of US $1.2 billion [52,53]. With the increasing popularity of electronic commerce, that is expected to exceed US$1 trillion globally [41], phishing is becoming more and more prevalent.

Online security, privacy and confidentiality are often listed as key concerns of customers in many surveys conducted in the field of e-commerce [21,35]. In a survey conducted by the European Electronic Messaging Association, 79% of interviewees indicated that security was their top concern [68] while 91% of online account holders expected stronger online authentication mechanisms offered by their service providers in a survey conducted by RSA [66]. The results showed that people were becoming more and more conscious about the safety of online transactions. It is believed that service providers who failed to address the security concerns might shatter the trust of their customers.

Banking industry is chosen as the target for this study. Banks generally perceive interruption, interception, modification, and fabrication as serious online threats [42]. Hong Kong is a major international hub of the financial sector and the headquarters of various financial institutions. With increasing use of broadband connections and Internet banking, Hong Kong has witnessed a growing trend in e-mail related frauds, especially during the holiday season [63]. Several phishing incidences that have occurred in Hong Kong have drawn the attention of the global financial sector [10,67]. 12 people were arrested in Hong Kong for stealing HK$600,000 in a phishing

* Corresponding author. Tel.: +852 2241 5845; fax: +852 2858 5614.
E-mail addresses: bose@business.hku.hk (I. Bose), alvincm@gmail.com (A.C.M. Leung).

0167-9236/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2008.03.001

scam targeted to HSBC in 2004 [67] and 14 suspects were apprehended by the Dutch police for hosting a phishing Web site similar to that of ABN AMRO Hong Kong in 2007 [50]. According to RSA's Monthly Online Fraud Report, Hong Kong moved from the third to the second position by hosting 15% of the reported phishing attacks related to US brands in April 2007. This was a significant increase over a figure of hosting only 2% of phishing attacks in February 2007 [8]. In this research, we investigate the preparedness of banks in Hong Kong in the face of potential phishing attacks. We study the variety of information related to phishing and anti-phishing measures provided by the banks on their official Web sites and provide judgment on the quality of the Web sites containing that information.

Establishment and maintenance of trust is very critical for businesses, especially online businesses, where the customers cannot verify the quality of products in advance [11,30,40]. Failure to establish trust may discourage customers from engaging in online transactions that risk disclosure of personal information [7,34,39]. Therefore, phishing is a major enemy of e-commerce service providers. Better preventive mechanisms against phishing are essential for all online service providers.

The primary objective of this research is to assess anti-phishing preparedness of banks in Hong Kong based on security information available on their official Web sites. We sought to answer the following three questions: (1) How well do banks present different types of anti-phishing information that can be categorized into phishing information and anti-phishing measures? (2) How do banks perform in terms of accessibility, usability, and content of this information? (3) What is the status of overall anti-phishing preparedness of banks?

2. Review of literature

This research addresses assessment of phishing preparedness of banks based on information available on their Web sites. In this section the literature related to this research is discussed under three headings. The various mechanisms of phishing attacks and the plethora of methods that are used to counter these attacks are discussed first. Next, we reviewed literature that established the criteria to be used for assessing Web sites. The following section justified the choice of metrics for assessment of anti-phishing preparedness, namely, accessibility, usability, and information content.

2.1. Phishing and anti-phishing

Phishing consists of several stages. Financial Services Technology Consortium (FSTC) decomposed the phishing lifecycle into six stages, namely, Planning, Setup, Attack, Collection, Fraud, and Post-Attack [74] while McAfee summarized it into e-mail retrieval, fraudulent e-mail generation, and harvesting personal information via malicious attachments, forms or Web site visits [71]. Phishing attacks can be categorized into malware, phishing e-mail, bogus Web sites, and identity theft. Malware is defined as programs that are designed to perform intentional unauthorized action [45]. Malware including virus, Trojan, and JavaScript code that perform cross-scripting attacks [31] is commonly used in phishing by attaching them to e-mails or embedding them in phishing sites to steal victims' private information surreptitiously. Anti-virus, anti-Trojan, and anti-keylogger are useful tools against them.

Phishing e-mail is another common channel of proliferation of phishing messages. Phishers pretend to be a trustable third party and send mass e-mail to the public and ask recipients to reply with confidential information or click onto an attached hyperlink leading to a phishing Web site. Gartner estimated that 2 million people had been enticed to release their sensitive information [61]. Another emerging trend is phishing attacks via Internet Relay Chat [47]. In order to deter such phishing attacks, one effective method is to adopt authentication of incoming e-mails [6], for instance, digitally signed e-mail for verification of company identity [25]. Many companies such as Cisco Systems, Microsoft, and Yahoo advocate mechanisms to authenticate source of incoming e-mails [49]. Mechanisms like Sender Policy Framework, DomainKey, and SenderID have been suggested for providing authentication [73]. Making use of alias e-mail addresses is also useful for minimizing the consequences [44].

The third channel of phishing attacks is via bogus Web sites. Phishers first build a Web site which looks very similar to that of a trustable third party and then invite the general public to log onto the bogus site by giving away confidential information for verification. In order to combat this attack, it is important to ensure that the digital server certificate exists for the site that is being visited. Measures such as trusted path ensured browsers are also useful to deter such phishing attacks [16].

After obtaining users' confidential information such as user name and password from an online banking Web site, phishers commit identity theft by impersonating the victim at the Web site of the bank they mimic. Two-factor authentication in the form of hardware security token, one time password and digital certificate, and zero knowledge proof are effective in deterring identity thefts. Table 1 provides a summary of the four types of phishing attacks and the possible anti-phishing measures that are adopted to counter them.

To better prevent phishing, both customers and companies have responsibilities to protect their own assets. Van der Merwe and Bekker outlined five anti-phishing strategies for service providers, namely, education, preparation, avoidance, intervention, and treatment [72]. Anti-phishing measures such as technology based tools (as listed in Table 1) and corporate

Table 1
Summary of phishing attacks and possible anti-phishing measures

Malware	Phishing e-mail	Bogus Web sites	Identity theft
– Firewall – Anti-virus – Anti-keylogger – Anti-Trojan	– Alias e-mail address – Digitally signed e-mail	– Digital server certificate – Trusted path ensured browser	– Two-factor authentication ≻ Hardware security box ≻ One time password ≻ Personal certificate – Zero knowledge proof