2011 International Conference on Advancements in Information Technology
With workshop of ICBMG 2011
IPCSIT vol.20 (2011) © (2011) IACSIT Press, Singapore

How Consumer Online Privacy can be Properly Managed

Rashad Yazdanifard [1,+], Zainab Bolanle Nurudeen [2]

[1] Centre of Postgraduate Studies,
Limkokwing University of Creative Technology,
Cyberjaya, Malaysia

Abstract. With the world now becoming a global village, most business have over the years migrated their businesses online commonly known as *e-commerce*. Though this new technology brings about a wider market reach and faster marketing for most companies, it has also raised the issue of trust between business owners and their customers. The customers want to be sure that their information will be kept private and also be conducted in a timely fashion accurately. The intention of this paper is to discuss the main issues concerned with consumer online privacy and how best to tackle these issues and possible technologies to address these issues.

Keywords – e-commerce, consumer online privacy, trust

1. Introduction

Following the rapid evolution of networks from the limited ARPANET to the multi-billion user internet, the world is now considered a global village and like villages go, trading, exchanges and other forms of human dialogue are indispensable. Reliance on the internet is now prevalent vis-a-vis mobile communication devices as well as social networking applications that interoperate on globally computerized platforms. [21] The internet is not owned by anybody neither is it controlled by any organization, Thus in spite of the best efforts of regulatory authorities such as the Internet Engineering Task Force (IETF),International Telecommunications union (ITU).,who develop protocols and guidelines for Internet use, the internet is indeed an open ground where various activities, nefarious and otherwise are abound. Following the above, there is the need to ensure the privacy of participants engaged in trade/contract over the internet. Privacy is the right of an entity to self determination with respect to the degree to which their personal details are revealed. [2]

Online privacy, loosely translated as internet privacy can be said to be the individual/organization's desire of personal privacy in matters concerning it over the internet. This desire can be further extended to exercise the individual/organizations right to determine exactly who can access their information and to what extent over the internet. The onus of providing this function rests with the service provider be it a bank, supermarket, government organization or an e-mail service provider. This is not to say consumers do not have a responsibility to keep their online particulars private as well as ensure compliance with online privacy policies of organizations. E-commerce sites, online banking applications, information warehouses and social networks are all but a few of avenues in which online privacy is required and are susceptible to compromise. There are various ways by which cyber thieves steal consumer identities online, Phishing being the most popular and successful one.

According to [9], Phishing is one of the many ways in which attackers retrieve information online through the creation of bogus websites by requesting for particulars such as usernames & passwords from

[+] Corresponding author. Tel.: + 60-173693170, +60-163505652
E-mail address: rashadyazdanifard@yahoo.com , zainab.nurudeen@gmail.com

consumers. There have been several celebrated cases of online privacy breaches which have resulted in identity theft thus leading to data loss, online fraud, trust exploitation and a myriad of other unsavory attacks.

A recent example in the Times Series Newspaper is that of David Peters, a man caught with 128 identities in the UK in July 2011.He used these identities to perpetrate frauds of up to £636,000.

Most Online users are prone to online identity theft the moment they have caused to transact any business online. Most websites have an online privacy notice which most consumers have failed to read. These notices are intended to promote consumer choice and reduce the risks of disclosing personal information online. But putting up these notices would have no effect if unread by consumers.

There are various online behaviors that may increase or reduce risk of online identity theft. This article will attempt to discuss the ways online identity theft occurs and help users understand how their actions online make them susceptible to these thefts and giving undue advantage to third parties to have access to their personal information.

2. Possible Threats to Consumer Online Privacy

Organizational efficiency is constantly endangered by multidimensional security threats. [20]. Compromise of consumer online privacy can be broadly classified as passive attacks and active attacks. Invariably the successful execution of the passive form of attack gives leeway to engage in an active attack.

Passive attacks seek information from a network system without altering the information either in transit or in-situ. Knowledge gained from the information gleaned can be used for purposes such as competitive pricing, technology stealing and other unfair leverages.

This form of attack is very difficult to detect as no information is altered and all seems normal. [24] Defined a passive attack as characterized by the observation/analysis of transmitted messages. The International Telecommunication Union, ITU in [14] consider passive attacks as exemplified in traffic flow analysis, release of message content, observation of data etc.

Various tools and utilities are used to carry out this form of attack. Among them are phishing, phreaking, skimming and pretexting.

Given that information security requirements of any organization must satisfy the cardinal demands of

- Confidentiality
- Data Integrity
- Data Authentication
- Access-control
- Non-repudiation
- Availability

3. Effects of Consumer Online Privacy Compromise

Based on [6] The rate at which customers participate in online surveys & related activities is highly hindered due to concerns relating to the privacy of their personal information. [8]. Effects of online privacy compromise could be felt socially, economically and politically.

The social effects include loss of trust and invasion of privacy, the economic effects include identity thefts and use of information while the political effects relate to Government use of citizens data.

Emergence of highly digitalised technological advancements have paved the way for government to introduce channels through which it could pass along information to its citizenry as well as exchange information with sister government agencies.

The deluge of information at its disposal which could include basic required information as well as secondary information thereby generating controversy amongst those concerned.This information is often regarded as private. Amongst the controversy generated are demands on the government to respect privacy concerns of the citizenry, the confidence of the citizenry in the government to securely keep their information, and the means by which (electronic or otherwise), communication with government takes place.[19]

- Identity Theft**:** Identity theft is a situation whereby data about an entity is obtained fraudulently in order to take advantage of a commercial relationship the entity has has with a service provider thereby empowering the thief to carry out transactions such as making purchases while the entity

(owner of the information) bears responsibility. [16] In the study carried out by Unisys (2009), In order of prioirity, identity theft followed by financial fraud was discovered to be of utmost concern for consumers. In fact, with reference to the banking industry, 75% of respondents would react to loss of trust issues by switching to other banks where better protection for privacy is guaranteed. [9] Recent cases of data breach is that of Sony Playstation Network where it was alleged that details of about 77 Million members of Sony Playstation Network are in jeopardy. Identities if not used directly by the thief to perpetuate harm is often placed on the black market for others to purchase. Research over the years has given an insight to the financial insight of stolen identities in the black market. A stolen identity costing $100 3 years ago, now go for as low as $14.[5] Andreas M. Antonopoulos attributes the sharp decline of price of stolen identity to an increased efficiency of the black market operations resulting in huge numbers of stolen identity thus the reduction in price. Online Fraud is an offshoot of Identity theft**;** annually, internet fraud is a cause for losses in consumer funds. There is a 57.43% increase in fraud related consumer losses between 2004 & 2005. [11].There are various types of scams that online consumers are susceptible to, one of them is the general merchandise fraud which is characterized by hijacking consumer purchases online so that merchandise purchased are not delivered to the buyer. Another type is credit card fraud which is perpetrated by theft of credit card details of an entity and making transactions in the card holder's name. An example of where this has been carried out is on the popular payment platform, PayPal. A spoof of the platform website was created & fed via email to customers requesting for detailed information such as social security numbers, date of birth, driver's license number, credit card numbers etc. [1]. Breach of consumer online privacy paves the way for online fraud to be perpetrated.

- Use of Information: Failure of information security measures is a cause of a number of security incidents. This failure could be due to technical reasons, managerial reasons, organizational reasons or human reasons. An example of organizations that have experienced inadequate security measures are choice point & time Warner. However, there are organizations such as Doubleclick & Amazon who considered it legitimate to make use of consumer information in their custody. [4] Failure to protect consumer information could lead to its exposure to unauthorized people; they could use this information to gain a marketing edge, technological advantage and other forms of unfair leverages. Also in the mix are third party sites that are present on sites used by parties. These third party sites gather information sometimes for marketing purposes without necessary due permission from the consumer. There are tools that enable users know if there are third parties present on websites they are surfing. These tools however, do not let users know what the third parties do with the information they gather. [7]
- Invasion of Privacy: The knowledge that his/her online information is susceptible to being viewed by a third party can create a psychological fear in the consumer. The fact that there are no recognized/standardized definitions of privacy hence weak laws protecting it further buttresses the consumers' fears. Inexactitude in the concept of privacy is a bottleneck. Hence it means different things to different people. By virtue of this the term "protecting privacy" is an unclear concept. [3]. In [15], it is said that lack of clearly defined legal policies to prosecute invasion of privacy is one of the many factors that has contributed to growing sensitivity to information privacy.[23], contributing to this invasion are consumer group lobbying activities such as those of electronic privacy information center. [22] The overall effect is the loss of trust of the consumer in the service provider system. The service provider could be an e-commerce site, a bank, payment gateways, gaming platforms and any other form of interface the consumer relates with. While there are many reasons that contribute to shoppers avoiding making purchases on websites, studies have shown that a fundamental reason is lack of trust. [10] In [18], corporate credibility which is composed of personal trustworthiness & expertise can be said to be the extent to which a company can deliver goods and services in meeting up with the consumer's expectation. [17][13]

4. What Security Measures can be taken to implement consumer online privacy

Companies should put in place stringent security measures to ensure consumer online privacy. These measures could be in different types. According to [9], measures both general & pervasive should inform an organizations security policy. Some of these measures are outlined below:

4.1. Education:

- Establish regular interactive sessions where employees are taught efficient security procedures.

- Websites can be used as a medium of communication in teaching employees online etiquette.
- Customers should be reminded to update relevant antiviral & antispyware software.[9]

4.2. Security department:

- There should be an autonomous security department with full fiscal control of itself.
- A 24/7 service desk in which identity theft and other related activities can be reported by customers.
- The office of the chief security officer who will be responsible for online security should be created.
- A security policy should be created and fully implemented.
- Internal auditors could be engaged as an extra measure. [9]

4.3. Constant monitoring:

- Agencies could be engaged to monitor activities on their websites.
- Following transactions, notification alerts can be sent to the customer probably via e-mail & preferably by SMS. This will enable the customer react immediately in the event the transaction is illegal. [9]
- Internal auditors could also be engaged.
- Monitoring of traffic, carrying out a traffic flow analysis and tracking of transactions would enable knowledge on who has access to the database. [9]

4.4. Security tools:

- Sensitive data should be encrypted using strong algorithms that cannot be broken. Unencrypted financial information should be closely guarded.
- Efforts should be made to assist users in identifying spoofed websites by making use of SSL & multi-layer security.
- Dual authentication procedures can also be implemented e.g. making use of session tokens for users.
- Email correspondence should be characterized by digital signature.
- The webpage interface the user uses could be affixed with an image selected by the user during initial registration. This would help the user distinguish it from a spoof site.
- Fraud detection can also be achieved using hitherto successful data mining tools. [9]
- Automated artificial intelligence measures can also be taken to detect subtle changes in online patterns & behavior. [9]

5. Cybercrime Impacts on Confidence of Consumers

Fig 1 below intends to illustrate relationships among the impacts of identity theft, use of information, and invasion of privacy as a result of cybercrimes and the counter e-security measures and policies taken to promote consumer confidence. [1]

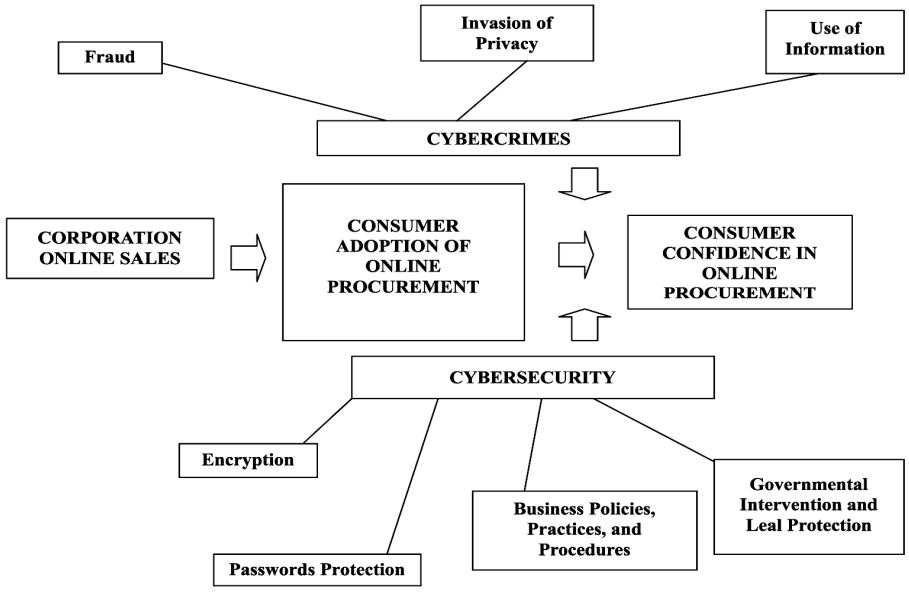

Fig.1.Proportioning forces connected with cybercrime and cyber security. [1]

6. Discussion

Consumer online privacy is an ongoing concern in the internet age; various techniques such as Phishing, Phreaking, and Pharming amongst others are used to gather information about consumers without their consent. Government and Private agencies responsible for the custody of consumer information have the duty to keep this information private and not disclose to any third party without permission from the consumer.

However, some agencies deem it their inalienable right to make use of information supplied them by their consumers. Identity theft, online fraud, invasion of privacy and loss of trust are some of the backlashes that emanate from consumer privacy compromise. There have been several cases celebrated and understated of this breaches. Various arguments have been raised on the legality or otherwise of the use of information obtained by breaching consumer privacy. One may look at the current riots taking place in the UK, it is widely acknowledged by the London Metropolitan police that some rioters coordinate their activities using social networking tools like Twitter, instant messaging application on the blackberry and post some of their activities on Facebook. Deputy assistant commissioner Stephen Cavanagh confirmed officers were looking at the websites (Twitter and Facebook) as part of investigation into widespread looting and rioting. It is suggested that they would achieve this by finding out personal details of suspects on these social Networking sites. There are also arguments on whether this form of evidence would be admissible in court on prosecution given the nature by which they were obtained.

7. Conclusion

This paper has examined consumer online privacy as an ongoing concern in the 21st century, as more users are added to the internet and more sites go live so does the risk of consumer online privacy breach increase. We have looked at the possible threats to consumers which include passive attacks like phishing, phreaking, skimming and pretexting. Also examined were the effects of consumer privacy being compromised such as identity theft, invasion of privacy and use of information. The various security measures that could be used to curb these various attacks have also being outlined to include proper education of staffs of organization on proper security procedures and also to inform consumers by putting up notice on the organization website. Having a dedicated security department for online security in an organization is necessary to ensure effective and dedicated attention to these threats. Effective monitoring of activities on an organizations website and employing necessary security certificates on a website are also methods outlined in this paper as a means to manage consumer online privacy. Consumer online Privacy is of very important concern to the consumers even to those who don't realize their information may have been leaked to a third party. Organizations should make this matter a priority so as to instill a higher level of trust in their customers and thus also increasing their own sales. Consumer Online privacy should not be looked down on by organizations, government and even social Networking Sites as these could result in loss of huge sums of money to the customers and also result in loss of trust in the particular organization which could possibly lead to their downfall if not properly managed. Proper Management of consumer online privacy would lead to increased trust in the organization by its clients who could translate into increased profitability. It's a WIN/WIN situation.

8. References

[1] Alan D. Smith, "Cybercriminal impacts on online business and consumer confidence", Online Information Review Volume 28 · Number 3 · 2004 · pp. 224–234, 2004

[2] Alan F. Westin, "Privacy and Freedom", Bibliography: p. 445-458, 1967

[3] Alessandro Acquisti, "Privacy and Security of Personal Information Economic Incentives and Technological Solutions", J. Camp and R. Lewis (eds), The Economics of Information Security, Kluwer, 2004

[4] Alessandro Acquisti; Allan Friedman; Rahul Telang, "Is there a Cost to Privacy Breaches? An Event Study" Twenty Seventh International Conference on Information Systems, Milwaukee 2006 and Workshop on the Economics of Information Security, Cambridge, UK, 2006

[5] Andreas M. Antonopoulos, "The black market for identity theft Security: Risk and Reward", Network World,

September 11, 2007

[6] Anthony D. Miyazaki, Sandeep Krishnamurthy, "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions", Journal of Consumer Affairs, Vol. 36 Issue 1, pg 28 – 49, Summer 2002

[7] Craig E. Wills and Mihajlo Zeljkovic, "A personalized approach to web privacy: awareness, attitudes and actions", Vol. 19 No. 1, pp. 53-73, 2011

[8] Culnan Mary J, George R. Milne, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices" Journal of Interactive Marketing, Vol. 18 Issue 3, pg 15-29, summer 2004

[9] D. Vijaya Geeta, "Online identity theft – an Indian perspective", Journal of Financial Crime Vol. 18 No. 3, pp. 235-246, 2011

[10] Enrique P. Becerra, and Pradeep K. Korgaonkar "The Effects of trust beliefs on consumers' online intentions", European Journal of Marketing Vol. 45 No. 6, 2011 pp. 936-962

[11] Francisco Munoz-Leiva, Teodoro Luque-Martınez and Juan Sanchez-Fernandez, "How to improve trust toward electronic banking", Online Information Review Vol. 34 No. 6, pp. 907-934, 2010

[12] Goldsmith, R. E. & Lafferty, B. A. & Newell, S. J. "The Impact of Corporate Credibility and Celebrity Credibility on Consumer Reaction to Advertisements and Brands". Journal of Advertising, Vol. 29(3). 43. 2000

[13] International Telecommunication Union, ITU, "Cyber Security guide for Developing Countries", Edition 2007

[14] Jochen Wirtz, "Causes and consequences of consumer online privacy concern", International Journal of Service Industry Management Vol. 18 No. 4, pp. 326-348. 2001

[15] Keith B. Anderson, Erik Durbin, and Michael A. Salinger, "Identity Theft", Journal of Economic Perspectives—Volume 22, Number 2—Pages 171–192, Spring 2008

[16] Keller, "Branding Perspectives on Social Marketing, Advances in Consumer Research, Vol. 25, Joseph W. Alba and J. Wesley Hutchinson, eds. Provo, UT: Association for Consumer Research, 299-302., 1998

[17] Mauricio S. Featherman; Anthony D. Miyazaki; and David E. Sprott, "Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility", Journal of Services Marketing 24/3 219–229, 2010

[18] Rowena Cullen, "Culture, identity and information privacy in the age of digital government". Online Information Review Vol. 33 No. 3, pp. 405-421, 2009

[19] Stephen C. Shih, "E-enterprise security management life cycle", Information Management & Computer Security Vol. 13 No. 2, pp. 121-134, 2005

[20] Wainer Lusoli and Ramon Compano, "From security versus privacy to identity: an emerging concept for policy design?" Vol. 12 No. 6 , pp. 80-94., 2010

[21] Waldmeir, P. , "Should americans exchange privacy for security?", The Straits Times, 2001

[22] Wijnholds, H.B. and Little, M.W. "Regulatory issues for global e-tailers: marketing implications", Academy of Marketing Science Review, Vol. 1 No. 9, 2001

[23] William Stallings. "Network Security Essentials" (Third Edition).