Journal of Accounting & Marketing
ISSN: 2168-9601

Muneer et al., J Account Mark 2018, 7:3
DOI: 10.4172/2168-9601.1000294

Mini-Review Open Access

Data Privacy Issues and Possible Solutions in E-commerce

Muneer A*, Razzaq S and Farooq Z

Department of CS & IT, University of Sargodha Sub-Campus Mianwali, Pakistan

Abstract

Privacy and security threats in the Information Sciences and data privacy have become a discussion topic among the users. E-Commerce is the part of Information Science; their users are not reluctant from the pain of data privacy issues and threats of security. If these privacy and security threats are not eliminated, users never trust, visit or shop at an E-commerce site. Maintenance of users' privacy online is one of the concerns of E-commerce. The usage of technical methods like cookies and capture their data has been raising the privacy issues since early past. This data mining is against the user's privacy under cyberspace. The paper attempts to give an overview of privacy issues and their possible solutions. We shall discuss the steps required before online shopping, and elaborate the purpose of privacy and security. A guideline is given to mitigate risks and vulnerabilities.

Keywords: E-commerce; Data privacy issues; E-commerce security

Introduction

Commerce is the continuance of business using the Internet with the help of web. E-commerce business becomes very popular now-a-days and comes into light with many privacy issues. As the result, users leave this platform, if these issues are not combatted, users will refuse to do online transactions [1].

E-business owners are exploiting the user's privacy for the growth of their business. Different authors have the different meaning of privacy as Etzioni belief that societally illegitimate and infeasible measure is defined as privacy [2]. According to Davies, it's a squandered right [3]. Experience shows that the users are concerned about the unauthorized access to their data. They never permit to reuse their personal data or sell it for the business purposes. Now-a-days online providers are specific on their privacy strategy [4].

The growth and trust upon E-Commerce business totally depend on the security and privacy policy of the site and for the development of E-commerce business most important factor is to build trust among users [5,6]. To maintain privacy in the E-commerce business, a complete and secure system is required [7]. Users feel hesitation in E-Commerce although online payment system is more secured and convenient [8].

Figure 1 shows the total number of reports that was registered as data privacy leaks from 2010 to 2017. It shows that in 2010 total privacy stealing cases were 662 and in 2011, it was 419. After this, it raised rapidly as 447, 614,783 reports appeared in 2013, 2014, 2015 respectively. In the recent years, data privacy issue became more serious as the numbers of incidents were increased from 783 to 984 in 2016 (Figure 1).

Privacy is a major issue in electronic commerce, as privacy enforcement and its monitoring are not easy. Some people consider privacy as the fundamental right and some people take it as the tradable commodity.

Figure 2 gives detail about data breaches from 2005 to 2014 in the United States.

From the customer's side, many e-commerce sites are doing silly activities with their personal data. According to a survey, there are 92% respondents told that although E-commerce site liable to keep personal data private but practically, they disclose personal things.

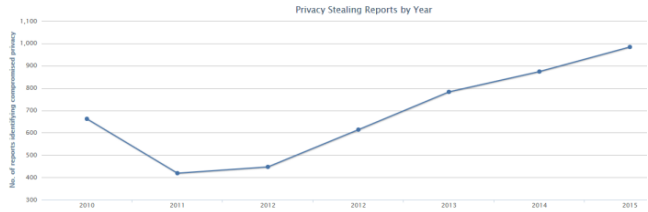

Figure 1: No. of reports registered against data privacy.

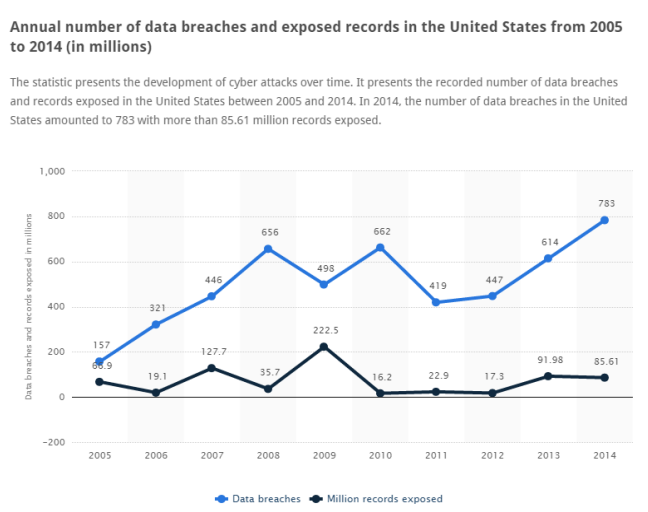

Figure 2: Data breaches in United State.

***Corresponding author:** Asia Muneer, Department of CS & IT, University of Sargodha Sub-Campus Mianwali, Pakistan, E-mail: aashiali33@gmail.com

Received June 01, 2018; **Accepted** September 05, 2018; **Published** September 13, 2018

Citation: Muneer A, Razzaq S, Farooq Z (2018) Data Privacy Issues and Possible Solutions in E-commerce. J Account Mark 7: 294. doi: 10.4172/2168-9601.1000294

Social and business issues

Privacy is a sensitive issue in the business context. We discuss privacy on the basis of technical issues and consumers' concerns. To capture data using digital systems and new computational techniques for data mining are easier. E-commerce sites are collecting the high amount of data related to customer preference, their buying patterns and the things they search at high volume [9]. Business analysts are using this data for the personalization of a customer's experience and for the improvement of e-site.

Use of personal data

1. The user's data is reuse for finding sales to existing customers and to know their interest patterns.
2. This data is used for aggregation and resale

From the customer's side, many e-commerce sites are doing silly activities with their personal data. According to a survey, there are 92% respondents told that although E-commerce site liable to keep personal data private but practically, they disclose personal things.

Kinds of privacy concerns

1. Consumers are concerned about unauthorized access due to security breaches.
2. They are concerned about secondary use – the reuse of their personal data such as sharing the data with third parties.

Data Privacy Issue

In the following section, we are presenting some of the data privacy issues, and attacking mechanism in relation to E-commerce.

Intellectual property re-selling

E-commerce business providers are freely resale the intellectual property of their customers. This is also an issue of the privacy of the individual using online trading sites and sharing their personal stuff without knowing the reselling rights.

Web activity correctness

E-commerce providers have no means to monitor the malicious web activities and its consequences.

Integrity of server machine

The E-commerce sites are not providing the mechanism for the client to verify the integrity of server machine.

Buyer' stricking

Social engineering techniques are used for the tricking of the shopper to get the maximum benefit of the under attacking system. The attackers gathers the credential details and use these against the online activities of the victim such as, asking about the user's favorite book is a common challenge question used by various sites for authentication and login to the account. If one of these sites is tricked into giving away a password after the challenge question is given, then the shopper used the same logon ID and password on other sites and possibly the site will be taken down.

Snooping the buyer's computer

One of the easiest way to get the control over the client credentials is to get the control over the computer of the online e-commerce user. As millions of computers are connected to the Internet every minutes and many of the user are unaware of the security feature and network vulnerabilities. Moreover, software and hardware vendors are not paying enough attention to guide about the security concerns of the devices and system, they are using. In this environment, it's very easy to snoop the computer of the e-commerce client.

Sniffing the network

Network sniffing is the attentive monitoring of the data between the shopper's computer and the server of hosting company. The attacker collects data about the buyer or steals personal information including credit card numbers, personal interest, buying pattern and etc.

Passwords guess

The guess about the user's password is in common practice. The password guess results the successful output using manual and automatic mechanisms. Manual method is more hard and has less success rate, and only result positive, when the attacker have the good knowledge about the victim as what are their liking, basic information about his/her family name, or the unique pattern the victim commonly uses. The automated method are quite fast, has high success rate and easy to perform. Many techniques including dictionary attack, and other tool exists that helps the attacker to guess the user ID/password combination.

Factors Affecting E-commerce Security

Role of computer auditing and log files

The role of log files and computer auditing is significant in e-commerce security as it stores all the data about the network activity. In the log files, a computer auditing program tracks the network activities including the files details such as, copied, moved, downloaded, or deleted; all successful and unsuccessful login attempts.

All the real-time online auditing of active Internet transactions is easily managed using the embedded audit modules. These audit modules are then further configured to some security measurement tool to evaluate the control risk. If any unusual activity is encounter, these log files automatically generate an alert, and send the report to the auditor for review [4].

Data Protection and Security

For the protection of data privacy, following steps are essential.

Alter password quickly

There are many chances to cheat the online users using some tactic. For the protection of privacy of user's data, online users must follow the practice to change the password quickly.

Avoid the same password at multiple sites

Never use a password which is already in use. Many E-Commerce site users use the same password for multiple E-Commerce sites. This gives a chance to access their account if anyone gets their account credentials from any other site.

Use the service of FAQs

An attentive study of FAQs is helpful before starting online process. Before placing the order, one should at least read FAQs for a lot of information which the user may not be aware.

Check site authenticity

To ensure the authority of the site, get the help from the search engine (Google, Bing, Ask, Yahoo). For the reliability of the users, this will help to authenticate the site.

Check site URL

Check website address before initiating the transaction. If the users are not checking the URL properly and placing the order at any similar E-Commerce site that looks like original, it may cause problems for the users after some time. The user should double check the sites' URL address and then should proceed for purchasing.

Avoid private data disclosure

The E-commerce site managers must avoid the discloses of private data to the other business information site. Many users voluntarily upload and share their private data to the E-Commerce site. This creates a chance that the E-Commerce site can use the private data for some other purposes without notifying their original user. Users should be trained and understand the importance of providing any personal data.

Fair data collection

A fair mechanism is necessary for the collection of data. The Internet usually makes use of cookies for data mining. This collection is not fair and suitable for data privacy of any user. The data user must have the knowledge of what personal data is collected and what is the purpose of its use.

Lawful collection of private data

A lawful mechanism must be followed for the collection of data. All the collected data should be utilized for the significant purpose.

Personal data utilization.

The use of personal data is significantly important and it must only be utilized for the purpose it is collected. After the completion of the motive for which data was gathered, it should be erased.

Data disclosure

Personal data never be disclosed to the person and without the main purpose, it is actually collected.

Personal data accuracy

The data user is responsible for taking all the possible steps for the insurance of data accuracy, relevancy and it is up-to-date.

Time for personal data retention

Personal data never be kept for the long period without significant purpose.

Duties of a data user

A registered data user is a person who controls, holds, and process the personal data". No one other than data user has the rights to access the personal data.

Rights of the users

Originator of the data has a right to access and prevent the collection of data from the person who cause damage. Nondisclosure of data must be strictly prohibited [9].

Conclusion

Privacy and security are the emerging issues in E-commerce. The paper discusses the privacy issues in E-commerce and provides a guideline to facilitate the users in doing the online transaction in a safe and secured mode. Currently, privacy is considered as a public issue, a proper mechanism is needed for the enforcement of data privacy in E-commerce. We mention some important precaution and security step that ensure that the users privacy is not at risk.

References

1. Budak C, Goel S, Rao J, Zervas G (2016) Understanding emerging threats to online advertising. ACM Conference on Economics and Computation pp: 561-578.
2. Lee I (2016) User Privacy Concerns for E-Commerce. IGI Global:Encyclopedia of E-Commerce Development, Implementation, and Management pp: 1780-1787.
3. Ackerman MS (2004) Privacy in pervasive environments: next generation labeling protocols. Personal and Ubiquitous Computing 8: 430-439.
4. Ackerman MS, Davis TD (2003) Privacy and security issues in e-commerce. New economy handbook pp: 911-930.
5. Smith R, Shao J (2007) Privacy and e-commerce: a consumer-centric perspective. Electronic Commerce Research 7: 89-116.
6. Corbitt BJ, Thanasankit T, Yi H (2003) Trust and e-commerce: a study of consumer perceptions. Electronic commerce research and applications 2: 203-215.
7. Lau RY (2007) Towards a web services and intelligent agents-based negotiation system for B2B eCommerce. Electronic Commerce Research and Applications 6: 260-273.
8. Castañeda JA, Montoso FJ, Luque T (2007) The dimensionality of customer privacy concern on the internet. Online Information Review 31: 420-439.
9. Kritzinger E, Smith E (2008) Information security management: An information security retrieval and awareness model for industry. Computers & Security 27: 224-231.