Security Issues For Online Shoppers

Dr. Abdulah Aseri

Abstract: In the present day, technology has transformed how human beings live and the processes they use to fulfill day-to-day activities. Buying and selling has been among man's key activities and over the years, these activities have become more sophisticated to enhance the ease and comfort of the experience. The shopping experience, buying and selling has further transformed over the past decade with the inception of the internet. Online shopping, and e-commerce in general, have gained popularity and provide more convenient and less stressful options transacting online. Consumers can now enjoy accessing products from distant stores according to their preference, a factor that gives consumers the ability to choose without considering distance and long queues. While online shopping promises to be a better option to the consumer, the channel is susceptible to threats, referring to elements that have the potential to inflict serious harm on a user's privacy leading to data breaches and a compromise of data security. As a consequence consumers are uncertain on whether to trust online shopping. This paper includes information on the threats of online shopping and highlights consumer perceptions, including negative consumer perceptions. The paper provides awareness on cyber security issues, including ways online shoppers and merchants can protect themselves from data breaches and attacks through methods such as phishing and adware.

Index Terms: consumer perceptions, cyber security, e-commerce, online shopping, online merchants, shopping experience, threats.

◆

1 INTRODUCTION

The internet has advanced markedly over this past decade, especially as an agent of communication, marketing and entertainment. This exponential growth of the internet has however, led to new problems brought about by the collection of consumer information by online merchants, and dissemination to third parties. The consumer data accumulated online exposes important details to unauthorized personnel, which makes the consumer susceptible to threats which include but are not limited to phishing, internet fraud, online scams and malicious URL's. For instance, consumers who prefer using credit cards transmit their credit card numbers via secure channels. Considering that credit cards are one of the most used payment criteria online, any compromise with a user's credit card number may prove fatal to the security of this information. Apart from the threat of exposing consumer credit card numbers, consumers also leave important information as they look for items from different online merchants. This research paper includes various ways e-commerce set ups can be compromised and the security measures that should be put in place to enhance the safety of online customer data. E-commerce is further burdened by the belief held by many consumers, of being too risky, with some considering the threats such as interception of important information by a third party. The paper also highlights various consumer perceptions of online shopping, including consumer perceived risks and how they inhibit the success of ecommerce as well as offering recommendations on ways negative consumer perception, with respect to e-commerce, can be addressed.

2 OVERVIEW OF ONLINE SHOPPING

The practice of purchasing products online has become popular because of the convenience that comes with the ability to have products on an online platform that can be accessed regardless of the location. Online shoppers can avoid queues and select the cheapest deals without having to walk around a city. E-commerce merchants, who sell their products exclusively over online platforms, and online sellers who buy commodities and sell them online for a profit, have reaped from the soaring heights of the internet's popularity in the 21st century [1]. These online merchants and sellers include provisions for various online payment solutions within their platform that encompass the features making online shopping and e-commerce in general, an attractive prospect. While online shopping seems convenient, it is susceptible to data breaches through methods such as hacking. Consumers therefore are reluctant when trusting online platforms since online channels are a threat to their privacy.

3 PERCEPTIONS OF ONLINE SHOPPING AMONG CONSUMERS

The internet's application in buying and selling has elicited various perceptions from people. Some find it being a better option compared to manual shopping because it is more convenient. Brick and mortar institutions are limited in terms of accessing the whole breadth of a country and consequently, having an impact. On the contrary, online shopping and merchants present their product portfolio to different people across the globe thus availing commodities that would otherwise prove difficult to access [2]. Online shopping therefore, thrives following the perception that they enable access, efficient search, evaluation, transaction and finally possession of commodities. Understanding consumer perceptions helps online businesses tailor their activities and improve returns from e-commerce sales. Online shopping is also subject to negative perceptions that prevent it from being fully embraced by internet users. The nature of online shopping makes it susceptible to third party interceptions, and as a consequence, it is considered as one of the riskiest buying and selling avenues. Most users do not trust the measures taken by ecommerce merchants to safeguard important information such as credit card numbers. Others also perceive online shopping as expensive and prone to delays when delivering the ordered products. Consumers also prove to be reluctant to purchase a product they cannot verify personally. Some perceptions concern with online shopping are positive while others negatively impact the acceptance of online shopping in the society.

- *Dr. Abdulah Aseri is currently an Assistant Professor Department of Management Information System, College of Business Administration, Imam Abdulrahman Bin Faisal University, Saudi Arabia, PH-133332101. Email: amaseri@iau.edu.sa*

4 THE FACTORS AFFECTING THE PERCEPTIONS OF ONLINE SHOPPING AMONG CONSUMERS

The perceptions of consumers towards online shopping are at times affected by their lack of understanding of cyber-attacks. These perceptions are influenced by:

4.1 Personality

Human characteristics vary and some people can lean more toward newer technologies while others prefer completing tasks traditionally [2]. Risk perceptions on online shopping also vary and this is especially affected by an individual's inherent ability to accept change and the accompanying risks.

4.2 One's inclusive social systems

Where the actual levels of risk remain ambiguous or unfamiliar to online shoppers, they rely on recommendations from others within the social system. These include friends, neighbors and relatives. Awan et. al. [2] supports this deduction as they claim that information on a new product or innovation is communicated through some channels over a period of time, within members of a social group. These channels include the press, newspapers and other mass media who dispense information such as data breaches at a quicker rate. The media's interpretation of an experience affects the experience's perception among members of the society.

4.3 Knowledge

Consumers fear that important information such as the credit card number can be accessed by unauthorized individuals when shopping online. However, it is evident, as presented by Schivinski and Dabrowski [3] that cases which have been reported, arose due to weaknesses in the design of the merchant's website. Furthermore, while reports by Maurer et. al. [4] imply that e-commerce is the riskiest buying channel, facts show that online transaction fraud has a lower prevalence when compared to fraud rates experienced in offline transactions [2].

4.4 Experience

The Consumer's experience also affects his or her perception. Customers who have tried purchasing items online are likely to repeat the same if the method proves trustworthy. The possibility of purchasing an item online is directly proportional to one's experience.

4.5 Shopping Context

Traditional shopping setups function in such a way that a consumer can see whoever they are dealing with. As a consequence, the consumer is confident that financial items such as money or a credit card number are delivered to the intended merchants. Online shopping does not have the advantage of face to face interactions which is the basis of trust in various partnerships [5]. This explains the perceptions held by consumers with respect to the levels of risk inherent in online shopping. The next sections highlight the actual risks online shoppers are susceptible to.

5 SECURITY THREATS TO ONLINE SHOPPERS

Online shopping has eased the consumers experience to the point that you can buy a product from the comfort of your home. The prices presented are competitive and products are mostly genuine, capped with offers during festive seasons. The dangers of engaging in online shopping remain unknown to most users leading to false perceptions of online shopping.

5.1 Phishing

One of the most prevalent security breaches affecting online shoppers are executed through phishing. As the name purports, a user is lured into giving his or her important passwords and credit card details using a click bait. Phishing is a situation where fraudsters transmit emails which they falsely claim to be affiliated to highly reputed firms so as to extract an individual's personal data. Phishing uses disguised emails as its main weapon, the goal being to trick a user with an urgent message such as a request from the user's bank requiring the user to download a form [6]. The malpractice can be categorized according to the user's intentions. It can be done to extract important information from the client, by tailoring a message to resemble a bank. Phishing can also lure a user into downloading malware, the files usually come with .zip extensions or Office documents embedded with malicious code, ransom ware is one of the most common malicious codes and has been detected in 93% of phishing emails [6].

5.2 Fake Online Stores

The internet harbors numerous online stores that convince people to purchase fake products, once purchased, these products are never availed to those who ordered them. These stores mimic the appearance of legitimate stores and in extreme situations, steal their identity.

5.3 Theft of data

Data theft has become an issue as online merchants accumulate important client information on their databases. System administrators and other workers who are authorized to access servers can access data without the owner's knowledge. A survey conducted by the British Retail Consortium (BRC) saw 62% of the respondents acknowledge data theft by system administrators and other workers as a threat [7].

5.4 Adware

A user can be bombarded with advertisements on online shopping platforms or social sites. These advertisements are at times illegitimate and they usually promise attractive rewards such as an iPhone 7. When the user clicks on an Ad, he or she is solicited for his or her personal details that can eventually be stolen by an unauthorized third party.

5.5 Identity Theft

Identity theft is fulfilled by paying attention to the activities undertaken by an online shopper. The crime perpetrators carefully monitor the activities of customers as they communicate with merchants via online stores so that they can be in a good position to masquerade as the merchants or online shoppers.

6 MAINTAINING PRIVACY AND SECURITY WHEN SHOPPING ONLINE

Most people like online shopping but the difficulty comes when safeguarding one's information. Online shopping is new to most consumers and trusting a new technology can take time, especially where money is involved. As more people embrace online shopping, malicious hackers also pervade the internet scouring for sensitive data. Therefore, users as well as online merchants should protect their details when purchasing items online. One way of ensuring your information is protected when shopping online is cross checking of the site your using is secure. This can be done by looking at the sites address, if the site address includes a HTTPS and not HTTP, then the site has encrypted your communication with a merchant thus preventing third parties from intercepting important details. These also prevents a user from opening fake online shopping stores than can infect a user when opened. These malicious online shopping stores extract important information after check out processes have been completed. Another precaution online shopper can consider when shopping online is the use of credit cards instead of debit cards. Credit cards have in-built defenses that are safer when compared to debit cards. Credits are connected to the bank's cash while debit cards are connected to one's bank account [8]. As a consequence, one's bank account is at a greater risk of being hacked when using a debit card. Moreover, encryption and validation techniques have ensured made the credit card comparatively secure compared to the debit card. Using one password for different online purchasing sites is risky. Online purchases are usually completed on different sites, therefore, using the same passwords for different sites makes one susceptible to fraud. Users should apply different passwords on different sites as they are the gateway to one's accounts. Unauthorized people can access passwords from insecure sites and use these passwords to inflict financial harm and invade the private lives of online shoppers. Phishing is the most effective tactic used by hackers to extract sensitive details from users. To prevent cyber-attacks through phishing, an online shopper should not open emails from ambiguous sources. In addition, when the bank needs some information from an online shopper, it would be prudent to call the bank before going forward. Online shoppers should also consider the security of the Wi-Fi connections they use to access the internet and online shopping sites. It is recommended that one should use his or her own Wi-Fi connection [9]. In case one has no other option other than using a Public Wi-Fi, then the individual should encrypt communication to prevent eavesdropping of financial data by fraudulent third parties.

A cyber security professional can address malicious attacks on the privacy and safety of data availed by online shoppers or merchants. Cyber security experts are well positioned to safeguard e-commerce from malicious threats that compromise the integrity of information. In most instances, the end user doesn't have the knowledge necessary to keep his or her information safe when online. A cybercriminal targets end-user as they interact on their phones and home networks. An action as simple as clicking on a pop-up feature can expose a home network, or a phone to cyber-attacks primarily due to lack of awareness.

7 PROPERTIES OF LEGITIMATE E-COMMERCE PLATFORMS

Online shopping sites that are recognized by the Better Business Bureau (BBB) are secure platforms (Miraz et al., 2017). When a user logs on to an online shopping site and encounters pop-up ads, it indicates an insecure site. Pop-ups have malware, adware and other malicious software. Websites that send emails without an online consumer's request could most probably propagate cyber-attacks. A consumer is only entitled to receive emails from known senders who the consumer expects messages from. Secure online shopping platforms can also be discerned by the presence or absence of contact information. If the online shopping platform includes an address, a telephone number, an email address and some key names affiliated to the site, then the site is more likely a trustworthy one. Companies that don't accept credit cards are not to be trusted since credit cards are well protected against frauds while debit cards are not. Online shopping sites that insist on the use of debit cards could most likely be having ulterior motives.

8 THE ACTUAL RISKS OF USING ONLINE SHOPPING PLATFORMS

Credit cards are widely used by online consumers and therefore, improving the confidentiality of credit card transactions will address some negative consumer perceptions with regard to online shopping. When transmitting information between an online shopper and an online merchant, the ecommerce server is usually protected by various protocols including the secure socket la (SSL) and the SSL-based Transport Layer Security (TLS) which is affiliated to IETF. A unique protocol named Secure Electronic Transmission (SET), is, as emphasized by Doloto and Chen-Burger [10], a fully integrated protocol which can secure a transaction from its initiation to completion. SET and TLS lower the risks of credit card fraud through applying effective cryptographic techniques unknown to the online shopper or end user. Consumer's perceptions however, are not informed by the stringent security measures made possible by TLS and SET protocols, and online shopping remains to be a risky exploit. A secure server which includes a firewall and precise information security policies set up by the network's administrators is relatively safe for online shopping. When the servers are configured poorly and there exists inadequate security policies, the confidentiality of stored consumer financial information such as the important details held by the credit at card are at risk. Connections to port 80, which are used by webservers, are usually open, hence rendering customer information insecure [11]. When firewalls are used for such connections, they analyze and record essential communication parameters on traffic within the network, including the incoming internet traffic. Firewalls hold details about the destination port and the destination I.P addresses attached to incoming traffic. Firewalls, should however, be well configured to prevent an instance where customer information stored in the merchant's server has been compromised [12]. Firewalls are limited since they only prevent attacks on the network through securing port 80. However, threats can come from other points of the network that are not protected by the firewallA variety of operating systems run e-commerce servers, these include Linux, Solaris, and Windows. These operating systems have differing security terms and levels of vulnerability. Linux and Windows 2000 differ in terms of features and security measures. In poorly configured operating systems, information can be vulnerable to malicious attacks [13]. The complexity of modern operating systems adds on the difficulty of avoiding loopholes within the OS design. Configuration should therefore be administered through running the latest security patches. With multiple operating systems (OS) in the market, it has proven difficult to establish a common standard dictating the preferred e-commerce server OS. This makes it difficult to avoid problems generated by accidents made when developing an OS. Web server applications are a necessary consideration when running a merchant server. Installing applications such as Apache, Cold Fusion and Netscape enterprise servers can protect an online shopper to some extent. However, these merchant servers are susceptible to attacks meant to compromise data stored in them. In 2010 for instance, Microsoft SSL ecommerce platforms contained encrypted transactions with trapdoors that enabled the cybercriminal to monitor systems [4]. As a consumer transmits payment information on forms provided by e-commerce websites, the Common gateway interface (CGI) acts as the interface between the user or online shopper and the server. However, while CGI offers some level of protection, it remains vulnerable since it is difficult to construct fully secure CGI scripts. Miraz et. al. [8] stipulate that the CGI can be a key source of security issues since they provide channels a third party can use to learn the system.

9 CONSUMER RISK PERCEPTIONS

When consumers purchase commodities online, they are unsure of the process and tend to attach online shopping to a number of risks. One of the consumer perceptions affecting online shopping is the failure of a product to meet the consumer's specifications. Despite the fact that such instances arise in brick and mortar settings, it seems more discomforting when it happens in online shopping. Online shoppers are skeptical because of not being in a position to assess the product's performance before making the purchase. The lack of a reliable method to test on the quality of products seen online remains to be a hindrance to online shopping. It is therefore prudent for online merchants to include online reviews of their products to educate online shoppers on the specifications of the product, including its advantages and disadvantages. 61% of the consumers read online reviews prior to purchasing a commodity [8]. The financial risk involved when engaging in online shopping has an influence on the level of acceptance of online shopping. Consumers are usually skeptical on the value of the product when compared to its price and revealing card information. Such instances of financial risk can be addressed by identifying a target market for your products while considering the income levels, which should be proportional to the price of the product. Furthermore, the site should contain multiple paying options since it is obvious that a consumer can buy what he or she is not in a position to pay for. Some consumers fear that shopping online can lead to time wastage. When an online consumer encounters a faulty product, or one that does not meet his or her expectations. The consumer can find the refunding process as time-wasting, even if there includes a money-back guarantee. An online merchant can avoid this short by applying the most convenient online delivery methods [14]. High prices affect the shopper's confidence negatively, and he or she will likely solicit for details from friends and product experts. An online merchant should practice guiding selling where the establishment provides as much information as possible, and personalized recommendations, especially when dealing with high end products. By providing sufficient information, an online consumer won't necessarily seek additional information on the product or online platform [15]. The information provided should however, be right information as customers will be attention on true and relevant details informed by an expert. Sellers use techniques such as online quiz to understand consumer preferences and increase their confidence by giving them sufficient information on the products preferred by the client.

10 THE ROLE OF GUIDING SELLING IN LOWERING PERCEIVED RISKS AND ADDRESSING UNCERTAINTY

Guiding selling addresses the functional risk through ensuring that customers are purchasing the right products for the intended purpose. The techniques also lower the financial risks through illuminating the benefits of a product and ensuring the customer does not pay for a feature that won't be of use to them [9]. The time loss risk is nullified by giving fast and professional advice when needed and ensuring that customers purchase the right products. This will prevent instances whereby the product is faulty and needs to be returned making the transaction convenient to both the online shopper and online merchant.

11 CONCLUSION

Online shopping is a new technique revolutionizing the shopping experience. Conventional shopping methods come with inconveniences such as long queues and a small range of items to choose from. Online shopping platforms are advantageous since they eradicate the need to physically appear at a physical shopping promise when one needs a certain commodity. Online shopping further enables more informed selection of the preferred models or products without indulging in frequent searches across stores. While online shopping proves convenient and less stressful, it is subject to malicious attacks from malware and other parties that compromise data safety, security and integrity. These attacks include but are not limited to phishing and adware techniques. As a consequence, there have been numerous data breaches which have also affected reputable firms such as Amazon and Google. Individuals remain hesitant when making the choice of whether or not, they can adopt online shopping because of rampant cases of fraud. Most fears are justified since online shopping involves financial transactions while some fears arise due to lack of proper information. By providing sufficient knowledge on cyber security threats that can impact clients, the security of online shopping via ecommerce sites will be enhanced and the accompanying awareness to end users will get rid of negative perceptions.

12 REFERENCES

[1] Baporikar N. Significance of critical success factors for Indian eBusiness. Transcontinental Strategies for Industrial Development and Economic Growth: IGI Global; 2017. p. 184-206.

[2] Awan JH, Memon S, Shah MH, Awan FH. Security of eGovernment services and challenges in Pakistan. Conference Security of eGovernment services and challenges in Pakistan. IEEE, p. 1082-5.

[3] Schivinski B, Dabrowski D. The effect of social media communication on consumer perceptions of brands. Journal of Marketing Communications. 2016;22(2):189-214.

[4] Maurer M, Firminger K, Dardess P, Ikeler K, Sofaer S, Carman KL. Understanding Consumer Perceptions and Awareness of Hospital-Based Maternity Care Quality Measures. Health services research. 2016;51:1188-211.

[5] Cheng Y-H, Ho H-Y. Social influence's impact on reader perceptions of online reviews. Journal of Business Research. 2015;68(4):883-7.

[6] Sandberg KW, Håkansson F. Barriers to adapt eCommerce by rural microenterprises in Sweden: a case study. International Journal of Knowledge and Research in Management and E-Commerce. 2014;4(1):1-7.

[7] Clarke R. Risks inherent in the digital surveillance economy: A research agenda. Journal of Information Technology. 2019;34(1):59-80.

[8] Miraz MH, Khan S, Bhuiyan M, Excell PS. Mobile Academy: A Ubiquitous Mobile Learning (mLearning) Platform. Conference Mobile Academy: A Ubiquitous Mobile Learning (mLearning) Platform. p. 89-95.

[9] Filieri R. What makes an online consumer review trustworthy? Annals of Tourism Research. 2016;58:46-64.

[10] Doloto U, Chen-Burger Y-H. A Survey of Business Models in eCommerce. Agent and Multi-Agent Systems: Technologies and Applications: Springer; 2015. p. 249-59.

[11] Hoek A, Pearson D, James S, Lawrence M, Friel S. Shrinking the food-print: A qualitative study into consumer perceptions, experiences and attitudes towards healthy and environmentally friendly food behaviours. Appetite. 2017;108:117-31.

[12] Lugmayr A, Grueblbauer J. Review of information systems research for media industry–recent advances, challenges, and introduction of information systems research in the media industry. Electronic Markets. 2017;27(1):33-47.

[13] Bouwman H, Molina-Castillo F-J, de Reuver M. Business model innovation in European SMEs: some preliminary findings. BLED. 2016.

[14] Salehan M, Kim DJ. Predicting the performance of online consumer reviews: A sentiment mining approach to big data analytics. Decision Support Systems. 2016;81:30-40.

[15] Gensler S, Völckner F, Egger M, Fischbach K, Schoder D. Listen to your customers: Insights into brand image using online consumer-generated product reviews. International Journal of Electronic Commerce. 2015;20(1):112-41.