EAI Endorsed Transactions
on Security and Safety

Research Article ICST.ORG

Prevention of crime in B2C E-Commerce: How E-Retailers/Banks protect themselves from Criminal Activities

Najlaa AlMajed[1], Leandros A. Maglaras [1,*], Francois Siewe[1], Helge janicke[1], Pooneh Bagheri Zadeh[1]

[1]De Montfort University, School of Computer Science and Informatics, Leicester, UK

Abstract

Online shopping and banking institutes are a current trend in e-commerce, where online shopping and banking are frequently used over the Internet. With the fast growth of the technology and on-line practices, criminal activities also have grown dramatically. Customer trust in the security of on line activities is extremely important for successful trading. Both buyers and sellers are vulnerable to online risks. With the current focus being on precautions that individual buyers and sellers should consider protecting themselves from criminal activities online, the issue of what e-commerce websites should do to minimize their customer's risk is apparently a neglected area in current literature. This research analyses deficiencies in online shopping and online banking websites, and identifies suitable procedures that e-commerce operators may apply to minimize the risk of criminal activities.

Keywords: E-Commerce, E-banking, Vulnerabilities, Protection

Received on 01 November 2015, accepted on 27 November 2016, published on 08 December 2016

doi: 10.4108/eai.8-12-2016.151727

1Corresponding author. Email: leandros.maglaras@dmu.ac.uk

1. Introduction

Electronic Commerce is about conducting business through electronic means, often over the Internet, between retailers and clients [1]. Electronic commerce provides convenience to the buyers as they can make online purchases from their home or workplace. Laudon and Travor [1] differentiate five types of e-commerce: business to consumer (B2C), business to business (B2B), consumer to consumer (C2C), peer to peer (P2P) and Mobile commerce (M-commerce). This research will focus on B2C, which is predominantly seen as 'online businesses selling to individual consumers [1]. Customers in many parts of the world utilize online services like e-banking and e-shopping. Online banking has been introduced in mid 90s and increased rapidly around the world [2]. Online banking offers electronic services that allow customers to check the balances of their accounts, transfer money in between accounts, pay bills electronically as well making investments. E–banking have a number of advantages compared to traditional banking since it is accessible twenty four hours, seven days a week without causing a journey to the bank sites or make customers wait in the queues. However, online banking can be unsafe and subject to fraud, as customers' details transfer over the internet [3], which introduces different risk exposure and privacy violations compared to traditional shops.

There are a number of benefits for customers when shopping online which are as follows: more choice of products than in a traditional store; easier to get to a specific store online rather than getting to a traditional store in a geographical area; less time consuming and sometimes customers can get products online cheaper than the products in traditional stores. Markham [4] stated that customers' trust in security in the mid-90s was not an issue, as peoplegave their credit cardsdetails over the phone to an organization, but their main concerns were about the way they make purchases by telephone or fax and/or the delay of payment or delivery. Markham [4] also further stated that in April 1995, there were around 27,000 websites, with its population doubling every53 days. However, a survey [4] by Herms showed a result of 62 per cent of the participates were thinking it is not advisable to give personal details through websites of online companies, where 60per cent did not make online purchases due to their concerns about security issues. In addition, the survey only includesfemales since they made the largest number of purchases. The results indicatedthat 75 per cent of women thought it was unwise to send their credit card details through online websites, where 75 per cent thought that they would not provide their credit card details because of security issues. Although there are many ecommerce users, the survey results showed a high percentage of the participants do not prefer using online activities and giving their sensitive information over the Internet. People may not want to provide their details over the Internet and/or give their information, simply because of the trust matters. Building trust between customers and online seller is a very important issue. Building trust in terms of securing the integrity and confidentiality of customers are one of the main area of concerns in e-commerce. [5].

Both e-retailers and customers are exposed to cybercrimes. Cross [6], defined cybercrimes as crimes undertaken over the Internet. It is also defined as a crime using a computer network for a criminal offence purpose. Further Cross [6] stated that both businesses and their customers lost millions of dollars caused by cybercrimes. Unfortunately, the cybercrime phenomenon is increasing year by year with new technology although security / computer professionals are trying to tackle these crimes [6].

The article makes the following contributions:

- Reviews how theft is affecting both e-banks/shops and their customers.
- Reviews the history and pros and cons of using e-commerce
- Explores how trust has been built between e-retailers/banks and their customers.
- Demonstrates examples of how cyber-crimes in e-commerce occur
- Looks at what preventions and cautions both parties can currently take into consideration to avoid cybercrimes.

2. The Increase of E –Commerce Crimes

New technologies have created new vulnerabilities, and hence increase cybercrimes and made security a bigger issue compared to a decade ago [6]. Internet users have more security awareness as well as software markets have produced more security products [6]. This does not mean that the Internet is safe to be used. Different users ranging from small, medium to large organizations and their customers need awareness about aware of cybercrimes. New security software increases in markets while new technologies that help cybercriminals to commit crimes increases as well. Cross [6] stated that 'cybercriminals love new technologies', including:

- Broadband
- Wireless
- Mobile computing and remote access
- Sophisticated Web technologies such as Java, ActiveX, and so on
- Fancy e-mail programs that support Hypertext Markup Language (HTML) and

Scripting

- E-commerce and online banking
- IM
- New operating systems'

Generally, the reason for the previous statement is that because criminals will have a larger space to play with, and less to learn [6]. Focusing on e-commerce and online banking technology, cybercriminals love this technology, because that is the place where transactions are conducted between businesses and consumers [6]. Besides, the famous bank robber Willie Sutton quoted "That's where the money is" when he was asked about the reason for robbing banks [6]. Customers give sensitive information, such as, banking details when conducting an online service like banking or shopping and this information could be saved on their PC, where it is not preferable to be used on a public PC. Internet users have been increased toover 3,100,000,000in 2015 [50]. When comparing cybercrimes today and a decade ago, the increase to the crimes is noticeable. This is caused by the ease of fraud commitment using email and websites [6]. Besides, as Soopramanien and Robertson [7] claimed that online shopping is an attraction for too many Internet users, to the extent that online shopping and traditional shopping are in a big competition. Hence, e-retailers/banks and their customers are in a perfect trap for cybercriminals. .

3. Customer Trust in E-Commerce Activities

The key to success in any businesses is customer trust. Customer trust in terms of security may not be effortless. Before the emergence of e-commerce services, customers could inspect the goods before making any purchases. The argument here is that customers buy products without checking and evaluating them and what makes them buy these products without inspection?

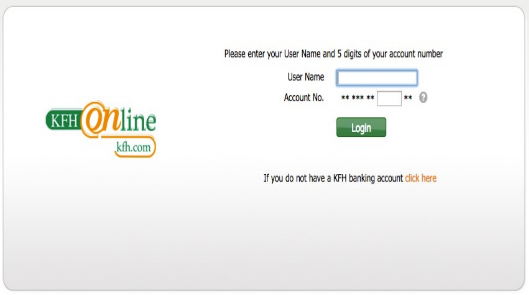
Reputation could be one of the reasons why customers deal with e-companies, whether they are e-banks or e-shops. A study on understanding of the customers' trust in e-commerce activities [52] suggest that security and transparency are the major issues in this area.

Further, consumers get their daily basics from traditional markets such as; medicine, food, cleaning supplies and so on [4]. Yet, things like fashion could be purchased online [4]. It has been argued by McKnight et al [8] that trust in an Internet retailer varies from one client to another. For some individuals trust depends on the feedback of others whom they trust [8]. Others may only use well-known and big organisation names, which have been used by many [8]. For example; Amazon.com and E-bay.com websites specialize in online shopping and are widely known amongst buyers [1]. Also, Hong Kong and Shanghai Banking Corporation (HSBC) is one of the most popular banks, is also being used by many clients. From the previous statement, it has been noticed that besides reputation and/or feedback, popularity in terms of trust is a significant issue. Why would buyers deal with unknown or inconspicuous organizations and put themselves at risk. E-marketing could play a big role in customer trust. E-marketing is defined as advertising products and services using the Internet [8]. The idea of marketing is to try to convince the audience on specific products or services and attract as many customers as they can. For example, repetitive banners or ads on well-known websites e-magazines/newspapers would build confidence in consumers; also a successful e-marketing plan is one trying to find customer needs. Williams and Page [51] studied the generations' needs in marketing terms and various marketing understandings and strategies appropriate to each generation's characteristics and behaviors, particularly in terms of segmentation, products and services, and communication. Further, customer experience and satisfaction could be essential in building trust, because when customers experience products and/or services this can lead to customer satisfaction.

Trust in e-banking is an important issue. According to Yab et al [9] the service quality in a geographical bank builds customer trust in online banking. Research presented by Yab et al [9] about trust in e-banking indicated the importance of reputation on the formation of trustworthiness in e-banking. Yab et al [9] also stated that clients would be confident in using online banking when they are satisfied with the services they receive in traditional banking. Therefore, it is noticed that building trust for online services not only depends on reputation, but also the quality of service in traditional banks is essential.

However, with reputation and quality of service it is still not easy to build trust in e-commerce. Usually, security and encryption are essential in terms of privacy protection [10]. Joseph-Vaidyan et al. [10] also argued that protocol needs to be created for trust purposes, since customers would then be more confident in using e-commerce activities. Also, it has been claimed by Joseph-Vaidyan [10] that there have been a lot of research researches conducted to define the term trust, where they find it complex and broad.

Security questions in online banking also help in building trust between e-banks and their customers. When customers want to login to their bank account they have to go through several security steps which makes customer feels more secured when using online banking. Besides their username and password, some banks would allow customers to choose a picture and a security answer, other banks may ask for the alternative password. For example; in Kuwait Finance House Bank (KFH), when a customer wants to log in, they must first inputs their username and 5 digits of their account number, the second step is to choose a security picture and inputs its description, then answering 3 different security questions, the final step is to input their password. The figures 1-1 to 1-4 below show these steps [11-14]:



Please enter your User Name and 5 digits of your account number

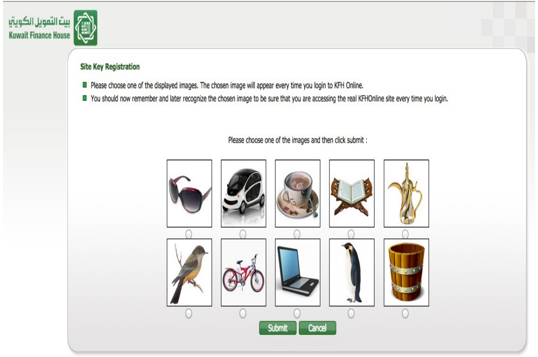
User Name

Account No. ** *** ** **

If you do not have a KFH banking account click here

Figure 1-1: Username and Account Number.

In the second step as shown in figure 1-2, customers should choose one picture and add a description for the chosen picture, when a customer logs in next time he or she must input the description of his/her chosen picture that will appear once they log in.



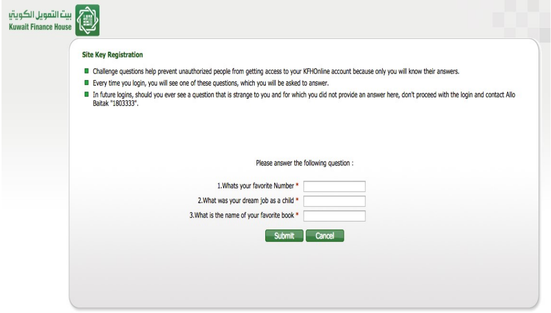
Site Key Registration

- Please choose one of the displayed images. The chosen image will appear every time you login to KFH Online.
- You should now remember and later recognize the chosen image to be sure that you are accessing the real KFHOnline site every time you login.

Please choose one of the images and then click submit :

Figure 1-2: Picture and Description.

In this step as shown in figure 1-3 customers should answer three different security questions, and every time they log in one question will appear and they must input a security answer that he or she answered, every time a different question will appear from the three questions every time he or she logs in.



Site Key Registration

- Challenge questions help prevent unauthorized people from getting access to your KFHOnline account because only you will know their answers.
- Every time you login, you will see one of these questions, which you will be asked to answer.
- In future logins, should you ever see a question that is strange to you and for which you did not provide an answer here, don't proceed with the login and contact Allo Baitak "1803333".

Please answer the following question :

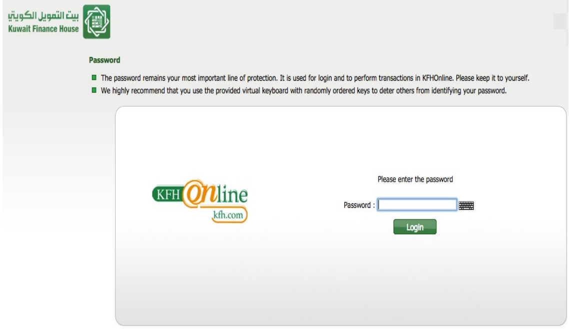
1.Whats your favorite Number *

2.What was your dream job as a child *

3.What is the name of your favorite book *

Figure 1-3: Security Questions.

The final step is where customers input their password, as shown in figure 1-4.



Password

- The password remains your most important line of protection. It is used for login and to perform transactions in KFHOnline. Please keep it to yourself.
- We highly recommend that you use the provided virtual keyboard with randomly ordered keys to deter others from identifying your password.

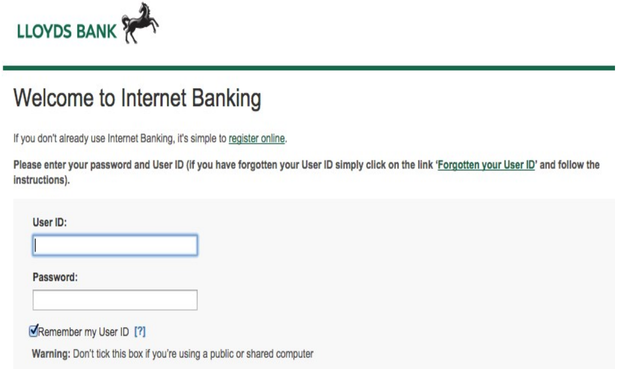
Please enter the password

Password :

Figure 1-4: Password.

Another example is Lloyds bank, when a customer logs in besides their username and password they must also provide a memorable password, but they have to give 3 characters whether it is a number or letter, for example they will ask for the third, fifth, and tenth character of the memorable password, and when they log in the next time they will ask for three different characters from the previous visits. Figures 2-1 to 2-2 shows each step in Lloyds bank.

The first step asks users to input username and password [15] as shown in figure 2-1.



Welcome to Internet Banking

If you don't already use Internet Banking, it's simple to register online.

Please enter your password and User ID (if you have forgotten your User ID simply click on the link 'Forgotten your User ID' and follow the instructions).

User ID:

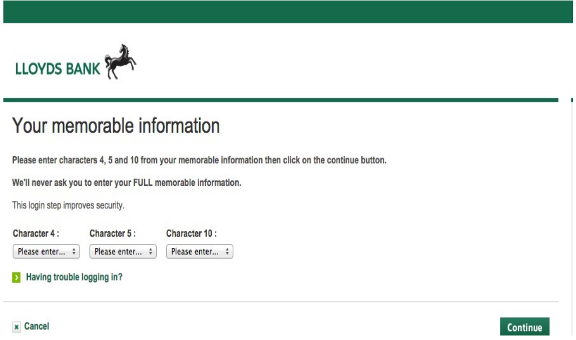
Password:

☑ Remember my User ID [?]

Warning: Don't tick this box if you're using a public or shared computer

Figure 2-1: User ID and Password.

The second step asks users to choose three characters of their memorable password [16] as shown in figure 2-2.



Your memorable information

Please enter characters 4, 5 and 10 from your memorable information then click on the continue button.

We'll never ask you to enter your FULL memorable information.

This login step improves security.

Character 4 : Please enter...

Character 5 : Please enter...

Character 10 : Please enter...

Figure 2-2: Memorable Information.

Further, in Lloyds Bank, when customers make changes in their online account a confirmation letter through e-mail will be sent to them and advising them to keep this email to realize between the real e-mail and fake emails and phishing e-mails.

4. Online Shopping

4.1.The Advantages of Online Shopping

Online shopping is an enjoyable activity, but only when consumers understand the key aspects of e-shopping. Online shopping may benefit too many customerswho have limited leisure time and allow them to view more than one department via one click. Online shopping benefits both businesses and consumers. Jia-xin et al [18] and Kacen et al [53] showed the advantages of online shopping. Firstly, there is no specific time or place for customers for e-shopping, as long as they are connected to the Internet they can shop whenever they want and wherever they want, which is less time consuming with less cost [18]. It is less time consuming since customers are not required to visit the geographical store and is also inexpensive. Further, they can also visit more than one store at the same time [18]. Secondly, customers have more choice of products than in a physical store, also, as the authors stated, some customers believe that they could find products which are not available in markets, in other words, unique goods [18]. Thirdly, customers could know the description of each item; the country of origin, how it functions, its price and features [18]. Finally, customers can purchase using a bank card, which does not take a long time; they would also get a confirmation email, which includes details of their purchase [18]. So, customers would not have to stand in a queue to pay. Also their details such as, name and address could be saved automatically. Online shopping has many advantages; however, there are disadvantages as well, which is discussed in the next section.

4.2.The disadvantages of Online Shopping

Both businesses and customers should be cautious while shopping online. The disadvantages that should be prioritized are security and privacy issues. In order to make an online purchase, customers must provide their personal details, which puts them at risk, since their information could be sold and/or traded between websites [18]. As customers pay online, security is an important issue, since hackers can attack websites and get customers' details [18]. Commenting on the previous statement, this would affect both businesses and customers, it would affect customers because it might destroy their accounts and for businesses they might lose their customers, because when an attack happens customers‘ trust would be effected. Another problem is; customers pay before the delivery of their products, which could be delayed or cancelled [18]. In this case, customers would ask for a refund if an item is cancelled, which might take time, as they have to contact their retailers about it. It is also a problem for businesses, because customers might make a cancellation when the product is already dispatched. Jia-xin et al [18] claimed that there are products, which should not be purchased online. It does not make sense when purchasing valuable items such as, gold, diamonds and luxury brands, which cost a huge amount of money. A further disadvantage is; customers cannot check the items texture, quality and size, for example, they cannot feel the material of clothes or see if the size fits them or not, as well as for food which they cannot taste [18]. Last but not least, there is no shopping atmosphere, some customers' shop not aiming to buy, but they might be more attracted too if they have chatted face to face with a salesperson and been convinced by their recommendations and advice for specific products [18]. Lastly, in physical stores customers can realize if this product is fine or damaged but it could not be realized online [18]. Kacen et al [53] claimed that Online stores have disadvantages with respect to shipping and handling charges, exchange/refund policy for returns, providing an interesting social or family experience, helpfulness of salespeople, post-purchase service, and uncertainty about getting the right item. They showed that advantages of online stores such as brand-selection/variety and ease of browsing do not entirely overcome the disadvantages. Even with the disadvantages of online shopping, people will still acquire goods from online stores.

4.3. Example of Criminal Activities in Online Shopping

Cybercrimes cost both businesses and consumers a lot of money. As Schneier [19] stated Willie Sutton robbed banks because it was the place where money can be found, but now money is everywhere diffused around the Internet. Fraud in online shopping could happen during a transaction. An example of fraudulence in online transactions that happened in 2006, which was reported by the FBI's annual report, said that there were 207,492 complaints, which caused losses of $198,492 [6]. Additionally, it has been argued in a conference in Ouro Preto that billions of dollars are being lost worldwide yearly from fraud cases in e-commerce [20]. For example; ebay.com, amazon.com and walmart.com are online shopping websites, that recorded a large number of online frauds; besides, fraud happens mainly on transactions [20]. Another example of online shopping fraud could be; a customer searching for a specific product in search engines and chooses a random website, registers and inputs the required information such as; name, address, payment details and so on; places an order then makes a payment and waits for the product to be delivered. But the order may not be delivered, because it is not a real online store with any items to sell. Rehman and Coughlan [21] claimed that fake websites are now quite widespread in online shopping. With fake websites people may lose money and sensitive information. There are many examples of online shopping frauds that caused losses for both e-retailers and customers. Avoiding online fraud and implementing the right security means is not easy due to variety of tools and techniques that cybercriminals use to steal money or sensitive information. These ways of theft could be unimaginable and mind blowing.

4.4. How do Criminal Activities Happen in Online Shopping?

In online shopping, both e-retailers and customers are targeted by cybercriminals, where they can get money and/or personal data. A criminal targets specific items in online practices. The main target for a criminal is the information of online users or shoppers [22]. Once cybercriminals get this information they could make transactions, steal money or make illegal purchases. When criminals use others' information for illegal purposes this might put the owner of the information in trouble. To get customers' information, criminals create fake websites, so when a customer wants to place an order he or she is required to give their information, and this information could be stolen or sold. Further, these fake websites might sell real items but at a low cost with the purpose of getting customer information. [21] claimed that one of the problem of online shopping is fake websites, since customers use their credit cards. Another purpose of a fake website is to steal customers' money. When a customer makes a purchase for items, their order might not be delivered. Schneier [16] suggested that the ease of committing a fraud by using personal data is a problem. It is always a problem when personal data is not secure, as it will lead to theft crimes and bad practices. Newman and Clarke [23] claimed that criminals target large businesses where there is a lot of money and information and can damage databases. The problem here is, customers would easily give their information because they believe that since they would give their details via telephone, there would not be a problem to give it away to e-commerce websites [6]. The previous problem shows how some customers do not take cybercrimes seriously and this might be a reason for the high number of cybercrimes. Yet, a phone call could be more secure since it would not travel around the Internet, and the call is between the caller and receiver. Cross [6] argued, it does not mean that this is confidently secured, a strike might happen but it is complex and expensive, also information would not be diffused around the internet. Pratt et al. [22] presented a study that showed that the majority of online shoppers do not believe threats in online shopping would affect them. Commenting on the previous study, the high number of cybercrimes does make sense and shows how people are complacent regarding the cybercrime issue, and this could cause online shopping fraud. Although there are a lot of security protection software products, yet consumers do not have enough awareness of cybercrimes.

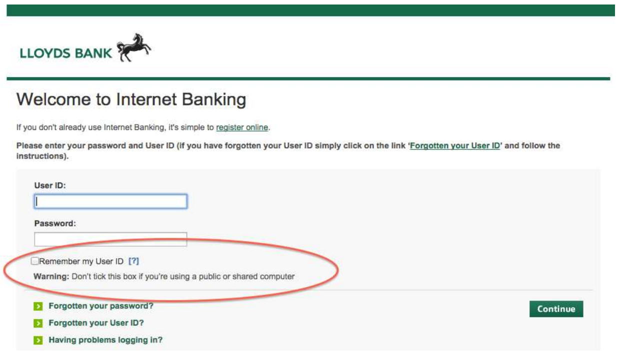
5. Online Banking

5.1. The Advantages of Online Banking

Banks have to invent a way to improve their products and services for their customers and to enlarge their businesses. The emergence of online banking has revolutionized the banking industry and made products and services more beneficial at a lower cost [3]. Online banking products and services have been used by many customers, who have benefited banks by enlarging their businesses and, as Verma et al. [3] claimed, online banking is the future of banks. If a bank fails in providing Internet banking, they will not survive [3]. Online banking services include; calculating interest, viewing and printing copies of statements, balance, checks and deposits, money transfers, bill payments, opening new accounts, stopping payments, updating via email from the bank and so on. Internet banking allows both customers and others to access their network [3]. When Internet banking allows public access this could get them new customers who know nothing about the bank and its products and services and when they have this information they may create a new bank account which would make it profitable for the bank. Online banking benefits both banks and their customers. For banks they may have more customers, since users could open a new account or use banking services from their home, workplace or while traveling without any effort, which makes it cost effective for customers as they would not need transportation to visit the bank physically. Verma et al. [3] discussed the main reason for online banking, which is; banks started to misplace their market share. With the appearance of e-banking, banks were able to stand on their own feet and continue in business. The reason for that previously stated is that it helped in market share reduction, provides more services to customers with lower cost and improved their image [3]. Banks want to introduce more customers to online banking since it will cost them less money. An online banking service is capable of finding accurate information quicker and easier than in the physical bank [3]. Customers do not have to stand in a queue behind the Automated Teller Machine (ATM) or behind the customer service counter in order to obtain some information about their accounts such as; balance available and statements. Another benefit of electronic banking for customers is that it is available 24 hours a day, and its services could be done through smart phones. Electronic banking could be more flexible than the physical banks, since customers would not worry about opening times as well as transportation to the bank. In addition, e-banking allows the customer to make international services with less transaction costs [3]. This also could benefit the bank if they have international customers and/or transactions for a better profitability. Advantages of using e-banking for the bank are, it offers competitive advantage, unlimited network, bank services can be anywhere if all branches are connected via a wide area network (WAN), it would be less load on employees in the branches, create a better customer relationship, and attracts more customers.

5.2.The Disadvantages of Online Banking

Although online banking is a way to expand the business and provides 24/7 online services, it has disadvantages. Mason [24] stated that the weaknesses of online banks as a system of e-banking are difficult and there is a third party between the bank and customer who could undertake theft practices. E-banking may need a full understanding from the customers of how it should be used in order to succeed in e-banking services. Customers could fail in using e-banking services, since they may use online banking on a public PC and forget to log out and/or save their details such as their username, where the online website usually advises customers not to save their username and password if they are using a public PC [15]. The picture below is an example of the previous declaration:



If you don't already use Internet Banking, it's simple to register online.

Please enter your password and User ID (if you have forgotten your User ID simply click on the link 'Forgotten your User ID' and follow the instructions).

□ Remember my User ID [?]

Warning: Don't tick this box if you're using a public or shared computer

Figure 4-1: Warning.

As can be seen in Figure 4-1 the warning message from Lloyds bank advising not to tick the box if the customer is using a shared or public computer. This is because if the customer ticked the box the user name would be saved, so whoever opens the same bank website next would find the username of the previous user appearing. Another disadvantage is; e-banks are not trusted by customers due to security issues [25]. Security could make customers use e-banking confidently, but security seems a large issue to some customers. Customer banking details are all around the Internet, which could be too risky for the customer and could cause theft. As Verma et al. [3] stated, "information of customers spreads around the Internet and it could be used for theft purposes". Shannak, R., O., [25] claimed that corporate customers have more trust in e-banking than individual customers. Hence, users of e-banking could be reduced due to the reluctance to use by some individual customers. Online banks could be hacked by cybercriminals and damage caused to its system and its database. Once the database is damaged criminals could rob the bank. Priya R. et al. [26] argued that hacking is one of the security problems in online banking. Besides hacking attacks, there are another cybercrime activities such as; phishing and malware [26]. Example of Phishing attack is sending fake emails representing a bank where they ask for personal details in order to deceive personal information from users to be used in illegal activities [27]. Users with no awareness may easily provide attackers with sensitive details not realizing this email is a trap. Malware is a program that breaks the computer's operation, and it has seventeen categories, e.g. Trojan horse [28]. The Trojan horse can be used to capture a user ID and password [26]. Once attackers get the user IDs and passwords all illegal practices could start. For example, money could be stolen, loans could be made, money transferred and so on. Customers must keep up with the information age, yet they have to be conscious of fraudulent activities and realize if this is a real or fake bank website. However, it is preferable that users use popular and well-known banks.

5.3.Examples of Criminal Activities in Online Banking

As argued earlier, cybercriminals cost those who are affected, both e-banks and/or customers, a lot of money. An example showed by Newman and Clarke [23] of electronic funds transfer fraud and that the information system and intelligence database of banks was the cybercriminals target with over 50 per cent of banks being affected by fraud. This means that more than half of the banks were victims to fraud activities, which is a large percentage. Another example is a hacking attack that happened in Los Angles banks and targeted specific information system or intelligence. The hacker, Kevin Mitnick, cost hi-tech companies an estimated $291.8 million [23]. In addition, in 1995 hackers cost businesses around $800 million and in 2000 the estimated cost was $1.6 trillion worldwide. It seems that not only businesses and their customers were affected, also companies who tried to protect banking systems. One example of credit card fraud is in Wales, where two British men targeted websites in the UK, USA, Canada, Thailand and Japan and stole credit card information from 26,000 accounts. These stolen numbers were sold in cyber markets of the former Soviet Union [23]. The losses for the previously stated crime went to over $3 million and globally, estimated losses, are in the billions [23]. In addition to this, 'Visa estimates that online credit card fraud accounts for 25-28 cents of every $100 spent, about four times worse than the offline rate of 7 cents per $100' [23]. Money laundering is an organized crime, with the aid of online banking and bank transfers and many other techniques, around 1 million dollars are laundered every year [23]. In investment fraud, criminals target customers who are cheated by false banks, which have used the web for transitional targets to accomplish fraudulent websites. Further, it has cost victims around $50 million [23]. It has been noticed that either individuals or a group of people does cybercrimes; yet, banks, customers and even governments have accrued a huge amount of money losses. Finally, an identity theft example that happened in the USA was done by a husband and his wife who worked together to steal the identities of vacant customers' bank accounts. They did this in over 6 US states . So, in 1997, 96 per cent of accounts of visa clients' bank credit card fraud caused losses of $407 million [23]. There are different and unimaginable techniques in online banking fraud, and when calculating the losses of all these crimes it could exceed trillions of dollars.

4.4.How Online Banking Crimes Happen?

In online banking there are different techniques for cybercrime. The aim for criminals is to get credit card bank account information, as well as hacking the banks database system and robbing the bank. Phishing is a technique used to online fraud activities, and it is categorised as malware, phishing e-mail, bogus websites and identity theft [29] Both phishing e-mails and bogus websites are considered as social engineering, where malware is considered as technical phishing.

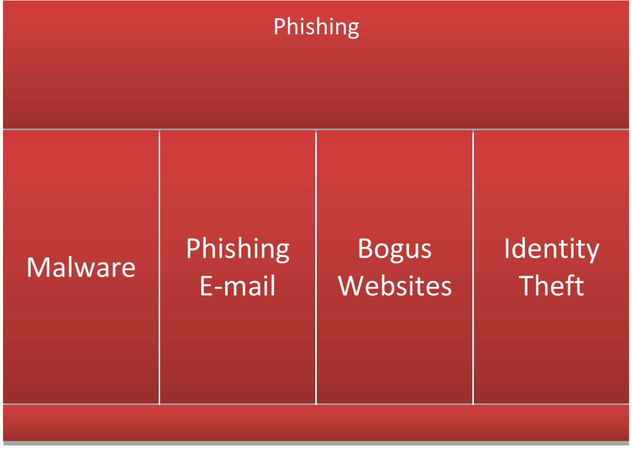


Figure 4-2: Phishing techniques.

Criminals use the technique of phishing e-mails by sending an email that represents a well-known organisation asking for users to provide sensitive details and to send them through email [29]. So users with no awareness might send their details and criminals could easily empty their bank accounts and/or use it for illegal practices. Another technique of cybercrime is malware, which includes, viruses and Trojan horse [29]. Malware and other malicious programs steal a user's privacy and can stop communication from the client before it reaches a bank [30]. Not all smart cards are protected yet; Trojan horse, worms and others could easily be used in an attack, because this will lead to the capture of PINs[30]. Hoar [31] stated that identity theft in the area of finance is growing swiftly in America and it aims to destroy personal identification, such as name, date of birth, Social Security Number (SSN) and bank credit cards. Identity thefts attack victim's new accounts, and checking accounts [32]. Finally, there is the bogus website technique, which invites people to log on into a website asking for confidential information [32]. So by this means all information is in the attackers hands and they may do unexpected and illegal crimes with this information.

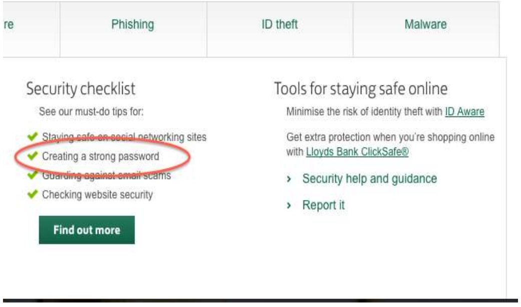
5. Preventions and Precautions E-Retailers/Banks and their Customers must consider

Online shopping and banking activities advantages are far beyond the disadvantages but only if e-retailers/banks and their customers know how to be protected from crimes. E-commerce activities are not secure, e-retailers/banks and their customers are advised to protect personal identification and databases to prevent cybercrimes. Information security fraud is the main issue in Internet activities [30]. In order to make E-commerce activities enjoyable users must try to reduce fraudulent risks. Information regarding security could be the most important issue in an organization. Killmeyer [33] stated the five components of information security, which are, organisation/infrastructure, policy and procedure security baseline of system components, security awareness and training, and compliance. It is not enough to install software security protection products; users should have security awareness. Also, e-retailers/banks should provide customers with information of risks that might happen during online shopping and/or banking. In e-commerce activities, user identification is always needed to complete a transaction in online shopping or to make online banking practices. User identification needs to be protected so that criminals cannot access other accounts, whether it's an online banking or online shopping account. There are many techniques that help in protecting user identification, which will be discussed in the next paragraphs.

Cryptography is a technique that should be used in e-commerce threats. Cryptography means allowing a secure message to be sent to an unsecure channel in order to assure their communication privacy [34]. Pfleeger and Pfleeger [35] claimed that cryptography is the strongest technique that controls different kinds of security risks. Cryptography consists of encryption and decryption, which are the opposite of each other [35]. Encryption aims to encode the message between sender and receiver, where decryption is to decode the message to its original form [35]. For example, when a client accesses his/her account the system understands the secret communication shared between customer and business [36]. In addition, Puente et al. [36] stated that the easiest and most used system is the login/password method, which identifies the users and allows them to access their account and check their profiles.

Security Questions is another technique for avoiding cybercrimes. Attackers may possibly guess the user's password and log onto their accounts, especially if the user used public pcs and saved their username. So, a username and password would not be enough to secure users accounts. Security questions, besides a username and password could be more secure, so hackers would not access the account easily. As Rabkin [37] stated, with security questions hackers could not access accounts easily.

Strong password could not be guessed easily if it includes different types of characters and is not similar to the username. Rabkin [37] mentioned that some banks ask users to create a strong password since this makes it harder for attackers to guess. Also, banks should renew pins, codes etc., which make the account much safer [36]. Some online websites and banks suggest users should create a strong password. For example, Lloyds bank advises their customers to create a strong password as shown in figure 5-1.



Security checklist

See our must-do tips for:

- ✓ Staying safe on social networking sites
- ✓ Creating a strong password
- ✓ Guarding against email scams
- ✓ Checking website security

Tools for staying safe online

Minimise the risk of identity theft with ID Aware

Get extra protection when you're shopping online with Lloyds Bank ClickSafe®

› Security help and guidance

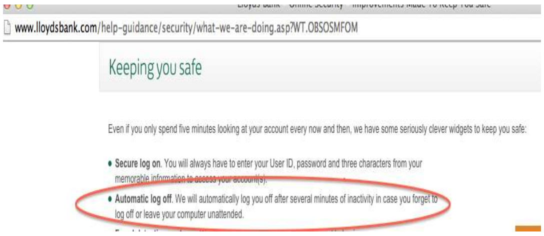
› Report it

Figure 5-1: Strong Password.

Adding mixed characters of letters, numbers and symbols could create a strong password. Further, while users create their password e-shops/banks could show them the strength of the password, if what they have created is weak, medium or strong.

Biometric system using fingerprints could be a useful technique, since it could be an accurate authentication of identification. Ihmaidi et al. [38] introduced biometrics as a security system for online shopping. 'Biometrics offers the means to identify individuals without requiring that they carry ID cards and badges or memorize passwords' [39]. Ihmaidi et al. [38] focused on biometric fingerprints and argued that it is a perfect technique for authentication, because fingerprints are very reliable and accurate. Further, the fingerprint-based biometric system could recognize twins who have similar DNA, since twins' fingerprints are not alike [38]. Also, the system provides a high level of confidence with positive verification. Fingerprint sensors could be rooted in devices such as in a keyboard and mouse [38]. Ihmaidi et al., [38] claimed that with a fingerprint-based biometric system online shoppers would feel more secure and confident in shopping online without worrying about online criminal activities. This system could be one of the most useful systems for the purpose of authorization because it recognizes the user from his/her fingerprint. In addition, this could also be useful for online banking practices to minimize the risk of fraud.

Automatic Log off is used by some banks, when a customer logs into their account, carried out some activities and forgot to log off or who had not performed any activity for a while, it would automatically log off. For example, Lloyds Bank [42] is using this technique as shown in figure 5-2.


Lloyds Bank - Online Security - Improvements Made To Keep You Safe

www.lloydsbank.com/help-guidance/security/what-we-are-doing.asp?WT.OBSOSMFOM

Keeping you safe

Even if you only spend five minutes looking at your account every now and then, we have some seriously clever widgets to keep you safe:

- **Secure log on.** You will always have to enter your User ID, password and three characters from your memorable information to access your account(s).
- **Automatic log off.** We will automatically log you off after several minutes of inactivity in case you forget to log off or leave your computer unattended.

Figure 5-2: Automatic log off.

This could protect users accounts if they logged in from public pcs, from their workplace or from Internet cafés.

Phishing Prevention is essential. Users should understand what phishing is, how to recognize a phishing email and how to deal with this problem. Anderson [41] claimed that phishing is a security engineering problem, since it is a mixture of authentication, psychology, operations and economics; also it is the fastest growing crime. Both banks and users should be aware of phishing emails and bogus websites. Phishing crime could attack customers as well as bank employees. There is an anti-phishing approach to prevent phishing activities [42]. Internet anti-phishing training tips have been provided for Internet users by organizations such as; eBay, PayPal, Amazon and HSBC [42]. There are two types of anti-phishing training tips; the first type is; tips for e-mails and the second type is for spotting phishing websites. Some anti-phishing tips will be shown on both, these tips being for both e-mails and websites [42]. The purpose of these tips is to teach users how to recognize phishing e-mails and websites. The first tip is that criminals usually include disturbing and astonishing statements in their (false) e-mails aiming to attract as many people as they can [42]. The second tip is that criminals usually ask for authentication information, such as, username and password, also, they ask for credit card numbers, date of birth etc. . The third tip is that e-mails from criminals are not personalized, but not always, where valid e-mails from a users' bank or e-commerce organization should be personalized and users must contact their e-retailers/banks to check if they are not sure [42]. The fourth tip is to not open any links from the e-mail that direct users to web pages, but it is advised that users contact their bank or e-commerce organization. The fifth tip is that talented criminals 'spoof' Http:// that users usually see on a secure web server [42]. So, users should not depend on the links that are displayed for them, they should check and search for the address of the e-bank or e-shop themselves [42]. The last tip showed that it is possible for criminals to forget the yellow lock, which normally appears near the bottom of the users' screen on a secure site [42]. If the yellow lock does not appear this means that the user is not on a secure or safe site [42]. If users double clicked on the yellow lock a security certificate for the site will be shown. Thus, users should not then continue if a warning has been displayed showing that the displayed site does not match with the certificate [42]. As previously discussed, users should be aware of links displayed in e-mails and not open it directly as this may lead to another new problem, which could be malware. Moreover, it is possible that these links include viruses that destroy user's PCs and when these PCs are hacked, criminals might get sensitive information. Therefore, it is also advised that users should use Ani-virus products to protect their PCs from these kinds of crimes.

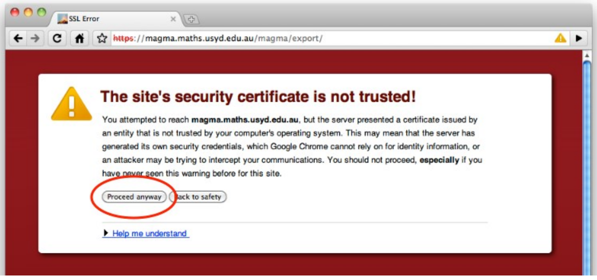
Security products could be essential for protecting databases. Database protection could be important for both e-commerce users and companies, because that is where the important data is. Awareness is also important besides the security products. In addition, attacks or virus actions could be through sending and receiving emails, downloading attachments, and all these kinds of activities [43]There are variety of security products like anti-virus, Intrusion Detection System (IDS) [49,54], firewall, Intrusion Prevention System (IPS), honeypots and so on [43] **Honeypot** is a resource, which is also able to get the hackers' details, which will be needed for evidence in court. Further, honeypot will make hackers waste their time and energy in trying to hack the system, but with no success, because the system is already protected [44]. Honeypot is categorised as; product-honeypot and research-honeypot. The purpose of product-honeypot is to protect the system from dangers by the attacker, while the purpose of research-honeypot studies the attack and helps in improving the detection system [44]. In addition, honeypot can be classified into low-interaction honeypot and high-interaction honeypot. "Low-interaction Honeypot is only based on the simulation of another host at a certain service, it's ability to interact with the intruder is limited; High-interaction Honeypot is able to provide a true interactive environment for intruders and has the ability to gradually increase the interaction with the invaders". Honeypot technology focuses on collecting data, since honeypot does not deliver real data [44]. Honeypot is used to collect new attack tools as well as attack methods. Yet, honeypot itself does not protect the system but it minimizes the risks with the defense of a firewall [44].

It is suggested that all organizations use honeypot to attract hackers and study and research new tools and methods of hacking as well as what the hacker is looking for. In addition, honeypot would provide data collection for the organization. Moreover, honeypot will decrease risks and protects the system, but it would not provide the system with full protection. Thus, organizations that are looking for a protection system that does not make them shut down the system are recommended to use honeypot to understand the risk that comes from the hacker and how it could be prevented.

6. Discussion and Findings

6.1 Lack of Awareness

In this research, it has been noticed that the advantages of both online shopping and online banking are far beyond the disadvantages. Yet, the disadvantages of e-commerce systems could be too risky. Further, not all users have full awareness of cybercrime, as many users believe that they are not the ones who are meant to be attacked in a cybercrime. In other words, users think, they are not the target for cybercriminals and this could be the most dangerous risk in e-commerce services. Lack of awareness is not only limited to customers, and employees should have awareness as well, since some employees were trapped by phishing as was shown in a case study earlier. Because of the lack of awareness many users are trapped by cyber-criminals. E-commerce activities benefit both e-retailers and e-banks in terms of profit, more product options and are less time consuming. However, users should be aware of fraudulent activities in order to benefit from online shopping and banking. Before using any online shopping and banking, users should check if the website is legitimate as well as the emails they receive which might be fake asking for personal and sensitive details. For websites, users should check for security certificates and it should be a trusted, security certificate warning [45] as shown in shown in figure (8.0) below.



The site's security certificate is not trusted!

You attempted to reach **magma.maths.usyd.edu.au**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

Figure 8-1: Security certificate warning.

Users should look at all the possibilities of cybercrime; in figure (8.1) it shows two options for users, they can either choose “proceed anyway” or “back to safety”, and it is advisable to choose “back to safety” because the other option could be risky for the user. For emails, some banks send an email advising the receiver to keep this email so they would recognise it as a phishing email; also, the bank emails include tips for users regarding awareness. Awareness could be more important than any security product; users should always have some information about new vulnerabilities in the technology world. Most importantly, some users should change their belief that fraudulent activities are not meant to be for them, that they are only for users with big accounts and/or organizations. A thief could steal a very small amount of money, for example they could steal 10 cents from many accounts and end up with a great deal of money. Furthermore, they could use the stolen details to make purchases, whether big or small ones, and many more purposes by stealing a user’s information. Therefore, the lack of awareness makes cybercrime attacks more likely to succeed.

6.2 Phishing Attacks

It has been noticed that phishing activities are happening a lot, especially when there is lack of awareness amongst users. These attacks could affect doctors, engineers, etc. Phishing is their greatest concern, because sometimes banks could not help their customers with the return of their money. Banks are trying their best to make users aware of phishing attacks but it still happens. Also, in the case study shown earlier about phone phishing, there was an experiment on bank employees and the employees were trapped by phishing emails. Bank employees, who were supposed to be more cautious than customers, had been fallen into this trap. So it means that not only bank customers were vulnerable to phishing attacks, even bank employees themselves should be cautious regarding this type of attack. In addition, to resolve this problem, banks should train and make more regular trials for employees to reduce phishing attacks. Attacks also could be done through a fake website that allowed shoppers to input their username and password and their bank details. Furthermore, there are some small details that differ from a real website and a fake one, but users may not notice these, or they may not even check if the website is real or not. Banks usually provide tips in the website, text messages and email and there were still people who were attacked by phishing crimes. Internet users should understand what a phishing attack is and how it happens. They should expect to get a phishing attack at any moment. Even if there is no money in a users’ account, he/she should be very cautious about it and have knowledge about phishing attacks to be able to protect themselves. Nevertheless, it is suggested that organisations should run a campaign about phishing attacks and share real stories of people who were trapped, instructions about how to spot phishing emails and bogus websites and how to be protected from these attacks.

6.3 Security

Bigorganizations, like banks and financial institutes, use a very secure system. Organizations face internal and external attacks and the internal attacks are more dangerous than the external, since the internal attacks come from employees who work within the system. In order to prevent the internal attacks, the bank should provide security ID for employees who work in the department of systems support management, front systems and channels, where they only have it during work hours and log into the system using the number shown in the security ID as shown in figure (8.2). When the employee enters the number provided he/she will be allowed to log into the system. Besides this, the number on the security ID [46] is changeable; it changes with every use, so the employee could not log in when he/she is out of the workplace.

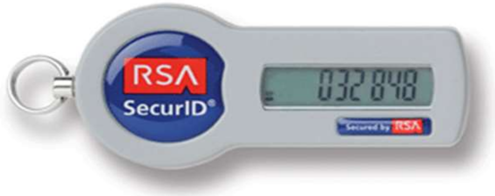


Figure 8-2: Security ID.

Security ID is useful for organizations in order to prevent internal attacks, so with this small device the organisation can secure their system, which does not allow anyone to login out of the workspace. Also, this device should kept securely. it should be always with the employee during work hours, because if this small device is left behind, it could be used for malicious activity. Another way for organisations to be more secured is to train employees frequently. Hacking is also a big risk in organizations. In a transaction, an attacker could make interruption either for the purpose of rational or for malicious. Further, attackers could immediately hack the organisation database or attack customers. In this case both sides need good security in order to prevent those third parties. So, security products like; firewall, anti-virus etc. are useful for both organisations and users. Furthermore, users should use up to date products to reduce harmful attacks. Furthermore, their organisations used high security, which is using additional firewalls from different brands. Hence, it would be more secure if users also adopted firewall in the server, which would decrease the possibilities of attacks. Online practices are not 100 per cent secure. In these cases, all users and organisations should try to reduce fraud attacks and should take it seriously, since the percentage of cybercrime is really high and is still increasing as shown in the earlier chapters. Also, organisations, governments and users have lost a huge amount of money because of cybercrime and security products. Using anti-virus for the server is a good way to give protection, where users can choose which emails they would like to receive and which emails they should consider to be spam. Also, it is suggested that when emails are in junk email it is not wise to trust it and move it to the inbox, because this could possibly be a spam email.

6.4 Trainingfor Employees and Managers

It has been shown that cybercrime could attack both customers and employees. This could be caused by lack of education in security. Education should be given to employees and managers periodically, since cybercrimes attacked different organisations, which caused them and governments huge losses. New vulnerabilities could arise any day, at any time, therefore, the organisation should prepare staff so that they are ready for any attack. Continuing Professional Development (CPD) should be given to employees and managers, since CPD is affective for staff in an organisation. "The maintenance and enhancement of knowledge, expertise and competence of professionals throughout their careers to a plan formulated with regard to the needs of the professional, the employer, the profession and society." [47]. As Council [47] stated, CPD improves skills and knowledge continuously, contains self-learning development, inventions of plans, updates to personal professional success and discovers the needs of the organisation and takes these into consideration.

Education is not only for beginners, it is also important for intermediates and seniors as well, because, as stated previously, new vulnerabilities could show up at any time, since being online is not 100% secure. All employees and managers should be educated about the possible cybercrime attacks that occur in an organisation to understand the environment of cybercrime.

6.5 Customer Trust

The key for successful businesses is customer trust. Engel [48] claimed that strengthening customer trust leads to a bigger business. However building customer trust is not that easy. In order to build customer trust, an organisation should choose the best strategy to make the customers feel able to deal with them. In addition, good service that is provided from an organisation is the strength of customer trust. Strength is; having more than a branch internally or externally which could be seen as trustworthiness amongst international businesses. So, this could make customers as individuals or corporations trust this organisation. As well as having a secure system for customers while using online banking, other protection such as encryption, sending security information emails and sending a text message after each transaction or payment has been done. Also, providing a good exchange rate for transactions could be another way of attracting customers trust. Marketing plays an important role in customer trust, seeing banners all over the websites and social networking websites could convince customers more, especially if these banners were well known and visited other websites. Moreover, good marketing and convincing customers about the quality of products are very important. Also, providing customers with lower prices than in traditional stores could attract more customers. In addition, a good marketing strategy is also using a technique to help build customer trust; yet, it needs to be really good because customers do not want to gamble with their money.

In online shopping, products could be delayed or not delivered, customers might receive the wrong goods, products could be delivered in a bad condition and sometimes the description of the product is different to the reality. In this case, the organization should provide refund and product exchange, as this will save the customer rights and give customers the flexibility to order again because they know they could obtain a refund or exchange if there is a problem with their products.

Using PayPal in some online shopping websites could be also a good idea, since PayPal enforces customer rights. PayPal is a payment service, which includes customer bank details and allows e-commerce shoppers to pay using their PayPal account, instead of inputting their bank details every time they purchase a product [48]. PayPal is simple to use with a cheap rate, which secures customers' payments [48]. PayPal is a protection service that is called "buyer protection" or "purchase protection" that requires no lawyer or additional costs [48]. If a website allows PayPal service, customers would trust this website, since they know in advance that their rights are protected and will feel comfortable using this on an online shopping website. It is suggested that users shop from online shopping websites that use PayPal, since it is a trusted service.

Customer trust is the most important matter in any business. Organisations could build customer trust in a short time or long time depending on their services, marketing strategies, feedback from others, etc. Customer trust in a traditional market could be easier than in an online market, since some online shopping websites maybe fraudulent. In order to build customer trust, organisations should follow a strategic plan that leads to customer trust; however, customer trust differs from one customer to another.

7. Conclusions

In conclusion, as e-commerce activities increase nowadays, cybercrimes increase as well. E-commerce activities have advantages and disadvantages, yet it is worth using it with caution. This research clarified what is cybercrime and what are the vulnerabilities of e-commerce activities. In addition, it showed how it affected e-commerce users and organisations and the huge losses caused by cybercrime. Furthermore, it showed solutions for retailers and their customers on how to prevent these crimes.

Cybercrime is an illegal action that is done via the Internet. Cybercrime includes; Internet fraud, online piracy, hacking etc. Cybercrimes are increasingly occurring; on the other hand, security products are being improved, based on the new attacks by cybercriminals. Besides this, new technologies, such as, broadband, wireless, mobile computing and remote access, have new operating systems and so are giving cybercriminals more and awider space to attack. E-commerce activities are a good technology for cybercriminals since customers provide their sensitive information to make online purchases or transactions and these sensitive details travel around the Internet. Researchers declared that the number of cybercrimes is much bigger than a decade ago; this is because Internet users are increasing each year. Besides, this puts the economy at risk because of the huge losses caused by cybercrimes.

Customer trust plays a big role in online shopping and banking. Customers prefer to use a safe website that provides services which satisfy customer needs. Further, customers use online banking based on the services they used to receive from their traditional bank. Additionally, reputation is important as well to gain customer trust and enlarge the business. For online shopping, websites that provide the PayPal payment method could be trusted more than websites that do not provide it, since PayPal protects the buyer and the purchase as well, is easy to use since it provides a quick payment without entering bank details for every new purchase and if there is a problem in the product or delivery PayPal will refund the money back to the customer without the need of lawyer or paying additional costs.

Online shopping provides a variety of products over the Internet, where there are many users interested in it. Online shopping has many benefits, since users could get more product options than in a traditional market with less cost and time and without the expenses of transportation. Online shopping can happen at any time and anywhere. Online shopping benefits organizations, since it enlarges the business. However, there are disadvantages of online shopping, which are; delivery delays, not able to touch and feel products and faulty products.

Online banking provides banking services using the Internet, which allows customers to view statements, transfer money and other financial services. Online banking benefits are; to use financial services at any time and from abroad, further, online banking services are available 24/7, during vacations and weekends. As the famous bank robber Willie Sutton said, the reason for robbing a bank is because there where the money is, this means that online banking has disadvantages as well, such as; phishing, hacking and Trojan horse.

Criminal activities in e-commerce target both e-retailers and their customers. For customers, cybercriminals mainly aim to get customers' sensitive information, where for organizations, cybercriminals aim to hack into their database. There are a large number of users who believe that they are not the ones meant to be attacked by cybercrime. On the other hand, billions of dollars were lost because of cybercrimes. The crime most occurring is phishing, which includes; malware, phishing e-mail, bogus websites and identity theft. In addition, phishing attacks worry organizations, since sometimes it might be too late for them to help their customers return back their stolen money. So, Internet users should be cautious and work on every possibility to prevent cybercrimes.

While Internet users are increasing, cybercrimes are increasing as well. In order to keep e-commerce activities enjoyable and beneficial, both e-retailers and customers must consider preventions and precautions to stay secure while practicing these activities. The Internet is not fully secure, yet users should still try to reduce e-commerce activity risks. There are many techniques that are available for customers to protect their user identification, which are; cryptography, security questions, strong password, biometric system, automatic log off, phishing prevention and security products. Cryptography is a technique that allows a secure message to be sent to an unsecure channel to make sure that the communication is private. The purpose of security questions is that even when attackers guess the password they could not guess the security questions and log into the account easily. A technique to secure the password is to choose a strong password that could not be guessed easily by others. An additional useful technique is the biometric system using fingerprints and this could be one of the best ways of security, because there is no possibility for any human being to have the same DNA. The biometric system is able to recognize the difference between twins with similar DNA. Another technique isautomatic log off that is been used by websites, which log off a user who has not used the system for a while, to prevent attacks from other people who do not own the account. One of the most important things is phishing prevention, where users have to have knowledge about phishing attacks in order to be able to recognize phishing emails and bogus websites. Additionally, security products, such as, anti-virus, firewall, honeypots and so on, are significant for a user's server, to prevent many types of attacks.

In the phone phishing analysis the study aimed to examine how employees answered the phishing email and the result was a surprise to the examiners, since the number of replies was higher than expected. This concludes that everyone who uses e- commerce activities is the subject for phishing attacks. Employees get training seminars periodically to prevent this type of fraud. Also, attackers are not only from external attackers, it is also from internal attackers, which are more dangerous since they have the system open to them. Last, but not least, big organisations like banks or financial institutes use very high security in order to keep their system safe by using the technology of high security and high availability and so on. Finally, all users, whether they are employees, managers and customers, should be cautious while using online activities, since new threats are very possible to arise online from now on.

References

1. Kenneth C. Laudon and Carol Guercio Traver, (2007). *E-commerce*. 3rd ed. USA: Pearson.
2. Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., Pahnila, S., (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Emerald*. 14 (3), pp.224-235.
3. Verma, S. B., Gupta, S. K., Sharma, M. K., (2007). *E-Banking and Development of Banks*. 1st ed. India: Deep & Deep Publications PVT. LTD.
4. Markham, J. E., (1998). *The Future of Shopping*. 1st ed. Great Britain: Macmillan Press LTD.
5. Kolsaker, A., & Payne, C. (2002). Engendering trust in e-commerce: a study of gender-based concerns. *Marketing Intelligence & Planning*, *20*(4), 206-214.
6. Cross, M., (2008). *Scene of the Cybercrime*. 2nd ed. United States: Syngress Publishing, Inc.
7. Soopramanien, D. G., & Robertson, A. (2007). Adoption and usage of online shopping: An empirical analysis of the characteristics of "buyers""browsers" and "non-internet shoppers". *Journal of Retailing and Consumer Services*, *14*(1), 73-82.
8. D Harrison McKnight, N. L. C. (2001). What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. *International journal of electronic commerce*, *6*(2), 35-59.

9. Yap, Kenneth B; Wong, David H; Loh, Claire; Bak, Randall, (2010). Offline and online banking - where to draw the line when building trust in e-banking?. *The International Journal of Bank Marketing*. 28 (1), pp.27-46
10. *Joseph-Vaidyan, K. V. (2008). Factors that enhance customer trust in e-commerce Web sites:*
11. Kuwait Finance House,. Username and Account Number. Retrieved from https://online.kfhonline.com/KFHOnline/appmanager/KFHOnlinePortal/LoginDesktop?_nfpb=true&_pageLabel=sitekeyPg
12. Kuwait Finance House,. Picture and Description. Retrieved from https://online.kfhonline.com/KFHOnline/appmanager/KFHOnlinePortal/LoginDesktop?_nfpb=true&_windowLabel=kfhOnlineLoginPt&kfhOnlineLoginPt_actionOverride=%2Fportlets%2Flogin%2FkF
13. Kuwait Finance House,. (2015). Security Questions. Retrieved from https://online.kfhonline.com/KFHOnline/appmanager/KFHOnlinePortal/LoginDesktop?_nfpb=true&_windowLabel=kfhOnlineLoginPt&kfhOnlineLoginPt_actionOverride=%2Fportlets%2Flogin%2FkFHOnlineLogin%2FenterImageCaption

14. Kuwait Finance House,. Password. Retrieved from https://online.kfhonline.com/KFHOnline/appmanager/KFHOnlinePortal/LoginDesktop?_nfpb=true&_windowLabel=kfhOnlineLoginPt&kfhOnlineLoginPt_actionOverride=%2Fportlets%2Flogin%2FkFHOnlineLogin%2FendSiteKey
15. Lloyds Bank,. User ID and Password. Retrieved from https://online.lloydsbank.co.uk/personal/logon/login.jsp?WT.ac=PLO0512
16. Lloyds Bank,. Memorable Information. Retrieved from https://secure.lloydsbank.co.uk/personal/a/logon/entermemorableinformation.jsp
17. Your registration has been successful. (2015).
18. Jia-xin, Y., Hong-xia, Z. (2010, November 7-9). *Research on the Advantages and Disadvantages of Online Shopping and Corresponding Strategies*. Paper presented at the IEEE Symposium, Henan. Doi: 10.1109/ICEEE.2010.5660278
19. Schneier, B., (2000). *Secrets & Lies*. 1st ed. Canada: John Wiley & Sons, Inc.
20. Caldeira, E., Brandao, G., & Pereira, A. (2014, October). Fraud Analysis and Prevention in e-Commerce Transactions. In *Web Congress (LA-WEB), 2014 9th Latin American* (pp. 42-49). IEEE.
21. Rehman, S. U., & Coughlan, J. (2012, June). Building trust for online shopping and their adoption of e-commerce. In *Information Society (i-Society), 2012 International Conference on* (pp. 456-460). IEEE.
22. Pratt, T. C., Holtfreter, K., Reisig, M. D., (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*. 47 (3), pp. 267-296
23. Newman, G. R., Clarke, R. V., (2008). *Superhighway Robbery*. 1st ed. United States and Canada: Willan Publishing.
24. Mason, S. (2013). Electronic banking and how courts approach the evidence.*Computer Law & Security Review*, *29*(2), 144-151.
25. Shannak, R. O. (2013). Key issues in e-banking strengths and weaknesses: the case of two Jordanian banks. *European Scientific Journal*, *9*(7).
26. Priya, R., Tamilselvi, V., & Rameshkumar, G. P. (2014, July). A novel algorithm for secure Internet Banking with finger print recognition. In *Embedded Systems (ICES), 2014 International Conference on* (pp. 104-109). IEEE.
27. Wu, M., Miller, R. C., & Garfinkel, S. L. (2006, April). Do security toolbars actually prevent phishing attacks?. In *Proceedings of the SIGCHI*

conference on Human Factors in computing systems (pp. 601-610). ACM.

28. Zolkipli, M. F., & Jantan, A. (2010, May). A framework for malware detection using combination technique and signature generation. In *Computer Research and Development, 2010 Second International Conference on* (pp. 196-199). IEEE.
29. Uusitalo, I., Catot, J. M., & Loureiro, R. (2009, June). Phishing and countermeasures in Spanish online banking. In *Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on* (pp. 167-172). IEEE.
30. Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today's online electronic banking systems. *Computers & Security*, *21*(3), 253-265.
31. Hoar, S. B. (2001). Identity theft: The crime of the new millennium. *Or. L. Rev.*,*80*, 1423.
32. Litan, A. (2004). Phishing attack victims likely targets for identity theft.
33. Killmeyer, J. (2006). *Information security architecture: an integrated approach to security in the organization*. CRC Press.
34. Coron, J. S. (2006). What is cryptography?. *Security & Privacy, IEEE*, *4*(1), 70-73.
35. Pfleeger, C. P. Pfleeger, S. L. , (2007). *Security in Computing*. 4th ed. America: Prentice Hall.
36. Puente, F., Sandoval, J. D., Hernandez, P., & Molina, C. J. (2005, October). Improving online banking security with hardware devices. In *Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on* (pp. 174-177). IEEE.
37. Rabkin, A. (2008, July). Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In *Proceedings of the 4th symposium on Usable privacy and security* (pp. 13-23). ACM.
38. Ihmaidi, H. D., Al-Jaber, A., & Hudaib, A. (2006). Securing online shopping using biometric personal authentication and steganography. In *Information and Communication Technologies, 2006. ICTTA'06. 2nd* (Vol. 1, pp. 233-238). IEEE.
39. Negin, M., Chmielewski Jr, T. A., Salganicoff, M., von Seelen, U. M., Venetainer, P. L., & Zhang, G. G. (2000). An iris biometric system for public and personal use. *Computer*, *33*(2), 70-75.
40. Lloyds Bank,. Automatic log off. Retrieved from http://www.lloydsbank.com/help-guidance/security/what-we-are-doing.asp?WT.OBSOSMFOM
41. Anderson, R. (2008). Security engineering. Indianapolis, IN: Wiley Pub.
42. Alnajim, A., & Munro, M. (2008, November). An evaluation of users' tips effectiveness for Phishing websites detection. In *Digital Information Management, 2008. ICDIM 2008. Third International Conference on* (pp. 63-68). IEEE.
43. Baroudi, S., Ziade, H., & Mounla, B. (2004, April). Are we really protected against hackers?. In *Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on*(pp. 621-622). IEEE.
44. Bao, J., Ji, C. P., & Gao, M. (2010, October). Research on network security of defense based on Honeypot. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on* (Vol. 10, pp. V10-299). IEEE.
45. Magma,. (2010) *Using Chrome*. Retrieved from http://magma.maths.usyd.edu.au/magma/faq/sslcertificate
46. Words of Wisdom from the Elder,. (2007). *Setting up RSA Secure ID on Windows Mobile*. Retrieved from http://keithelder.net/2007/10/03/setting-up-rsa-secure-id-on-windows-mobile/
47. Council, G. D. (2013). Continuing professional development. *Online information available at http://www. gdc-uk. org/Dentalprofessionals/CPD/Pages/default. aspx (accessed December 2011)*.
48. Engel, M., & Stark, J. (2013). The CESL as a European Brand-Paypalizing European Contract Law. *Available at SSRN 2246271*.
49. Leandros A. Maglaras, Jianmin Jiang, "A novel intrusion detection method based on OCSVM and K-means recursive clustering", EAI Transactions on Security and Safety, vol. 2, no 3, e5, pp. 1-10, January 2015.
50. Internet users (2015), http://www.internetlivestats.com/internet-users/
51. Williams, K. C., Page, R. A., "Marketing to the generations." Journal of Behavioral Studies in Business, *Vol. 3,* pp. 1-17, 2011.
52. Colesca, S.E., "Understanding Trust in e-Government", Journal of Engineering economics, Vol. 3, pp. 7-15, 2009.
53. Kacen, J. J., Hessa, J.D., Chiangb, W. K., Bricks or Clicks? Consumer Attitudes toward Traditional Stores and Online Stores, Journal of Global Economics and Management Review, Vol.18, pp. 12-21, 2013.
54. Leandros A. Maglaras, Jianmin Jiang, Tiago Cruz, "Integrated OCSVM mechanism for intrusion detection in SCADA systems", IET Electronics Letters, Volume 50, issue 25, December 2014, p 1935-1936, DOI: 10.1049/el.2014.2897