DOI 10.7603/s40601-014-0019-3

Security Awarness Program for Customers Using Online Banking

Khulood Al Zaabi and Abdallah Tubaishat

Received 20 Aug 2015 Accepted 17 Sep 2015

Abstract -- **Due to the increasing demand on electronic payments, fraud methods are also increasing which has resulted in the loss of millions of dollars worldwide each year in the banking sector. Several studies have been conducted to counter against fraud in the banking domain and to come up with ways to secure online payments. None of these studies, however, have resulted in a comprehensive awareness program which targets customer banking. The purpose of this research is to propose an awareness program, Information Security Awareness Program, dubbed ISAP. We believe that such a program is needed for the following reasons: a) in order to enhance the level of trust in online banking, b) to protect each customer's personal information and c) to comply with the online bank requirements. We have identified several online frauds, and then we recommended some best practices for online protection in the following areas: online shopping, online protection, password protection, operating system protection, identity theft protection, and debit/credit card protection.**

Keywords– Online Banking; Awareness; Security; Card Fraud; ID Theft; e-Banking; Corporate Account Takeover.

I. INTRUDUCTION

E-banking is an electronic way of delivering both new and traditional banking services and products directly to customers. Online banking provides financial institutions, individuals, customers and businesses permission to access their accounts and transact business. It also provides related financial products and services through each bank's web site [15]. With regards to the bank's developments (online banking), by using secured electronic transaction technologies, all customers can access services such as credit/debit/smart cards, Electronic Funds Transfer (EFT) system, and Mobile banking easily from anywhere and at any time [15].

As a massive volume of banking and monetary transactions have been occurred through the internet, using devices such as laptops, tablets, and mobile phones, online banking customers have become a playground for cyber criminals. Therefore, it is critical that online customers are aware of how to protect their electronic assets, their sensitive data and personal identification (ID).

There are three major pillars of a Cyber Security Program: technology, process and people [2]. People, which we call customers, are the weakest pillar among the three which require more attention to protect them from cyber-attacks.

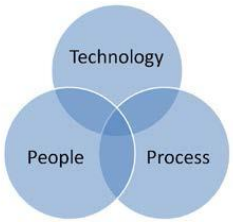

Figure 1 The Three Major Pillars of a Cyber Security Program

Banks expect from customers to have a firewall, an anti-virus and an anti-spyware program installed on their devices, as they hold the responsibility for any financial loss. However, a large number of online customers fall into phishing attacks which lead to lose a significant amount of their money. Banks refuse to refund those customers because they think that this is the online customers' responsibility which leads for loosing valuable customer as well as business [9].

II. LITERATURE REVIEW

The main objective of reviewing the literature is to highlight crucial information which may shape up the content of the proposed ISAP for online banking. The related works to this study are addressed as follow:

DOI: 10.5176/2251-3043_4.3.334

Published online: 13 December 2015

A. Identity (ID) Theft and Prevention

Identity theft has become one of the most famous forms of thefts in the United States as millions of Americans have been affected in the past few years [1]. ID theft victims didn't find that they were victims for months or years after the crime. Also, the credit reporting bureaus have spent a lot of time and energy in recovering victim's unfortunate incidents. Abdullah's research [1] discussed what identity theft is, how it does occur, and mentioned the two types of identity theft which are: "Account Takeover", and "Application Fraud". He indicated that the consequences of identity theft are as follows: the thief starts to gather the victim's personal information such as date of birth, name, address, phone numbers, social security number and driver's license number by different styles like stealing, mail fraud and phishing. Moreover, his research explains how identity thieves use acquired personal information which can be done by calling the issuer of the credit card and impersonate the cardholder in order to ask to change the account's mailing address, or to open a new account using the victim's personal information. He concluded by saying that after months or even years, victims discover that they have been a victim of identity theft either by receiving a call or a letter from the collection agencies to ask them to pay their debit. After the victims have discovered the crime, they are advised to follow the following steps in order to recover their loss. Firstly, they should contact the banks and creditors, change his/her account PIN codes and passwords, and record all the names and phone numbers that they corresponded with when they discussed their case and lastly, to return all original reports. Despite all of these efforts that the customer takes, in some cases the credit card agencies or even the banks do not believe the victim and believe that the customer is trying to get out of paying their debts. The researcher refers to this as "repercussions of identity theft on the customers". Abdullah suggested minimizing identity theft by providing and encouraging customers to follow the following steps:

- Encourage customers to request a copy of their credit card report from the credit reporting bureaus
- Encourage customers to keep up-to-date the passwords on their credit card and phone accounts
- Encourage customers to secure their personal information at home
- Encourage customers to ask about information security procedures in the workplace
- Encourage customers to never give out their confidential information through phone, email, or over the internet unless they are sure about who is calling or they are the ones who initiates the conversation
- Encourage customers to shred any documents that contain confidential information rather than throwing it into the trash
- Encourage customers to update their anti-virus, anti-spyware and to use hardware or software firewalls

B. Security and Usability

Most traditional banks are now offering online banking services and encourage their customers to access their online banking website with "peace of mind", because they claim that they provide their customers with comprehensive guidelines as part of their efforts against internet-based attacks. These guidelines have been examined in terms of security and usability by major Canadian banks [9]. It was found that the guidelines were higher than the regular customers understanding level and they noticed that some of the marketing-related messages about safety and security were actually misleading to the users.

Most of the banks advertise "free" anti-malware products on their websites, and they encourage online customers to adhere to the following instructions [9]:

- Install and maintain up-to-date security programs
- Review related user agreements including online banking, client card and privacy agreements
- Keep the Operating System (OS) and browser up-to-date with security patches
- All passwords and Personal Verification Questions (PVQs) for online authentication should be unique
- Promptly reset online banking passwords over the telephone or on a trusted computer after accessing online banking websites when using a public computer
- Distinguish real emails from phishing by looking for their personalized email messages. For example, the customer's real name should appear on the message as several banks nowadays provide a secure message center for sending important messages/notifications to their customers
- Not to provide Social Insurance Numbers (SIN) or similar identity numbers to others

III. WHY ISAP FOR CUSTOMERS

The purpose of this research is to propose an Information Security Awareness Program (ISAP) for online banking customers to enhance the customer's trust of online banking, and to guide customers how to safeguard their confidential information from being used in identity theft, electronic fraud and other common threats encountered by today's online banking risks. The research approach is to educate online customers of how to deal with internet theft in the banking sector, and remark tips into how to secure internet banking. The research study begins with describing ID Theft methods such as Phishing, Vishing (Voice Phishing), Smishing (SMS Phishing), and debit/credit card fraud to online banking customers and how to prevent these risks. Furthermore, the study describes the Corporate Account Takeover and how to prevent it. Finally, we conclude this study by recommending some online banking security best practices.

Despite the fact that nowadays corporates have the best and intelligent firewalls with encrypted web traffic using https Secure Sockets Layer (SSL), hackers can still attacks their confidentiality through the Corporate's customer devices. Online banks enforce their online customers to sign a comprehensive online banking security terms and conditions, but these terms are not clear for some customers as they aren't equal to their education levels. If online customers fall under one of the digital crimes, such as identity theft, they will blame their online banks. This can potentially result in the customer losing trust in online banking and impact on the bank's reputation. Furthermore, online customers face multiple information security threats such as phishing and social engineering. Recently, hackers have been using all of these threats in order to attack their targets. It is therefore imperative, that banks make their online customers aware about information security threats and implement countermeasures for their devices as well [8]. This research addresses all of these threats and related countermeasures, by proposing information security awareness for online customers which can help minimize or eliminate security threats.

IV. ONLINE BANKING RISKS

A. Identity (ID) Theft

According to Newman and McNally [10], the Internet has played a major role in spreading information about identity theft in terms of risks and informing individuals of how they can avoid victimization. Because of anonymity in the cyber world, cyber thieves have become skilled in maximizing their chances of targeting victims. However, there is a difficulty in conducting scientific research on identity theft because of a huge number of different crimes that are being committed which include: the use or abuse of others' identity or identity-related factors such as cheque fraud, plastic card fraud (credit cards, cheque cards, debit cards and phone cards), terrorism by using false or stolen identities, and other kinds of theft such as pick-pocketing, and burglary in order to obtain the victim's personal information. In the following sub section, we intend to give brief information about identity theft, including definition, types, and stages.

1) ID (Identity) Theft Definition

Identity theft is composed of a number of disparate kinds of crimes committed in varying venues and circumstances [6]. According to Abdullah [1], identity theft has a negative effect on the victim's credit history, and has created serious financial hassles for the victims as it involves the unlawful acquisition of the victim's name, address, date of birth, social security number, mother's maiden name, driver's license and bank or credit card account numbers. Identity theft crime permits the thieves to use the victim's information and attempts to duplicate the victim's identity to open new accounts under the victim's name, purchase automobiles, apply for loans or credit cards, and get access to social security benefits.

2) Types Of ID Theft

There are various types of identity theft; the most common theft is credit card fraud of various kinds. Credit card fraud has increased on the Internet and telephone due to the opportunity provided by the Internet environment. Credit card fraud can be discovered quickly by the credit card issuing company, often before the cardholder is aware that the crime is being committed and that is why some researchers prefer not to include credit card fraud as identity theft. In addition, there are other types of identity theft such as account takeover which takes more time to identify and investigate [6].

3) Stages of ID Theft

There are three stages of ID Theft which are acquisition, use, and discovery [6].

Stage 1. Acquisition of the Identity

The fraudster acquires the victim's ID through theft, computer hacking, fraud, trickery, force, redirecting or intercepting mail, or even by legal such as purchasing identifying information on the Internet [6].

Stage 2. Use of the Identity

For financial gain, the most common motivation is to hide one's ID from law enforcement or other authorities such as bill collectors, and to avoid arrest. There are many crimes under this stage such as [6]:

- Account Takeover.
- Opening new accounts.
- Extensive use of the victim's debit/credit card.
- Sale of the ID information on the street or black market.
- Insurance fraud.
- Stealing rental cars.
- Filing fraudulent tax returns for large refunds.
- Acquisition (Breeding) of additional ID-related documents like driver's licenses, passports, visas, and health insurance cards.

Stage 3. Discovery of the Theft

Evidence suggests that the longer it takes to discover the theft, the greater the loss incurred by the victims. As research indicates that ID Theft may take from 6 months to several years. However, some ID crimes may be discovered quickly [6].

B. Debit/Credit Card Fraud

Electronic payments by credit cards have several advantages such as purchasing online products or services from any country. However, it has many security risks, and therefore, credit card fraud losses are increasing daily.

1) Credit Card Fraud Definition

According to Al-Furiah and Al-Braheem [3], credit fraud is an unlawful usage of others' credit card, without informing the cardholder or credit card issuer. There is no relationship between the fraudster and cardholder. The fraudster has no intention to either inform the cardholder or make repayments for the goods which have been purchased. Credit card fraud has two types; offline fraud and online fraud. The online fraud takes place through mail, telephone or the Internet. On the other hand, offline fraud is a traditional way by using a stolen credit card at a store to purchase any item. Recently, there is a study that indicated that identity theft is being committed more frequently offline than online, which means that the online victims discovers the fraud faster than the victims who relied on offline paper bills or statement monitoring [6].

2) Types of Credit Card Fraud

According to Al-Furiah and Al-Braheem [3], credit card fraud has various types and it can be categorized as fake card fraud or skimming which has been a fast-growing criminal activity in recent years. Skimming constitutes almost 24% of the total credit card fraud, where a device is used to scan a card and obtain the code hidden in the magnetic stripe in order to replicate it and use it fraudulently. The second type is called a stolen card and constitutes almost 25% of the total credit card fraud. For this type of fraud it is necessary to obtain the details of the card without informing the cardholder in order to commit this type of fraud. The third type constitutes 21% of fraud and this is called Mail, Telephone, and Internet Order (MTIO). This type is considered to be the fastest among all types. The fourth type is the lost cards. This constitutes 15% of all crimes and is defined as a card that is reported as missing by the cardholder, or a card that was never received and lost in the mail. Customers consider the last type of crime as the least harmful. Moreover, customers should know Card Verification Value2 (CVV2) which consists of the three of four digit number printed on the front or back of the credit card. This is considered as a security feature to prevent fraudster activity. Even if someone obtains the credit card number from the Internet, unless he/she doesn't have a physical card, he/she won't be able to know the CVV2 value [3].

C. Corporate Account Takeover

According to Castell [5], online account takeover is an unauthorized person that gains online access to an existing bank (considered as one form of identity theft). This fraud occurs when an unauthorized party steals the account's access credentials and then conducts illegal transactions on it. The fraudster's target is the online customer's account, and the intention is to remove, steal, and procure funds of the targeted victim. Account takeover is achieved by using malicious software, which has the ability to exploit one entry point into the network in order to start the theft process. Moreover, fraudsters may use social interaction to prompt the victims into revealing account information which will allow fraudsters to gain access into their account and move the money out of the account in a short time. It is estimated that the losses from account takeover fraud of over $2.9 billion in 2012.

Corporate account takeover is a fast growing electronic crime where thieves typically use some form of malware to obtain login credentials to corporate online banking accounts and fraudulently transfer funds from the victims' account [5]. When fraudster intends to target the victim, he/she tries to send phishing email which directly names the recipient

correctly. This phishing email contains an infected file or a link to an infectious website. The victim will trust this email as it contains a trusted recipient's name who is generally a person within a company who can initiate funds transfers or payments on behalf of the business. When the victim opens the attachment or clicks the link to open the website, the malware will install in the victim's computer a Trojan keystroke logger, which intends to harvests the victim's corporate online banking credentials. The victim's online credentials are uploaded either to a website where the fraudster can download them, or the Trojan keystroke logger may detect this and immediately sends an instant message to alert the fraudster of the secure web activity, in case the bank and the customer are using the two factor authentication system. When the fraudster captures the victim's online username and password, he/she will try to access the financial institution or hijack the secured web session. After a while, the fraud is carried out when the fraudster tries to create a new account under the victim's name or initiates a funds transfer through wire acting as the legitimate user. After a couple of days or hours, money will be deposited and will be directed to the fraudster [5].

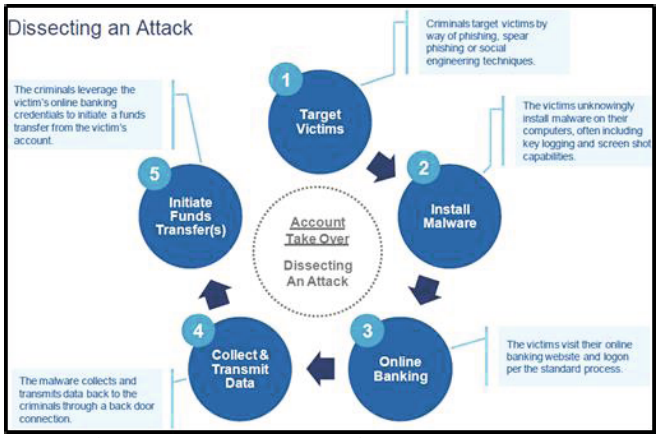

Figure 2. Corporate Account Takeover [5]

D. Phishing (Via E-mail)

Phishing is an identity theft fraud method. The fraudster tries to send an email that appears to be from a valid company which has a business relation with the victim. The email will request the victim to click on the attached link in order to redirect him/her to the website where they could update their information. This fake web site that the fraudster created collects the victim's information [1]. The fraudster can fake the victim into providing their Social Security Numbers (SSN), Internet banking credentials, financial account numbers, and other personal information. Thieves often position as:

- Financial institutions
- Credit card companies
- Utility or other biller
- Internet service providers
- Government agencies
- Prospective employers

Here are some clues to identify phishing e-mail [7]:

- The Phisher may address his/her victim with nonsensical greeting or may encounter an awkward greeting and refer to them in a non-professional manner
- In order to avoid email filters, the phisher uses a technique called "Typo & Incorrect Grammar", where the errors are intentional
- Source code points into fake websites instead of the real ones. Even though the link looks legitimate, when the victim moves his/her mouse cursor over the link, source code points into the fake websites
- The phisher tries to send "urgent call to act" email to encourage the victim to act immediately. The email usually threatens that the account could be closed or canceled by writing "We are updating our records", "We have identified fraudulent activity on your account", or "Valuable account and personal information was lost due to a computer glitch"

E. Vishing (Voice Phishing)

According to the City State Bank, the phisher attempts to call their victims or leave voice mails indicating that "Your personal account has been frozen" [7]. This message advises victims to immediately input his/her debit card number, expiration date, PIN, and CV2 (3 Digits security code) from the back of debit card. Then the phisher will use the provided information via a telephone for unauthorized ATM withdrawals.

F. Smishing (SMS Phishing)

Smishing is derived from "Phishing", and "SMS" comes from SMS which is the protocol used to transmit text messages via cellular devices. You do not have to use your computer to be vulnerable to online scammers [6]. Mistry, Dahiya, & Sanghvi [13] showed an example of Smishing; you may receive a SMS message saying that "Your debit card has been suspended, to reactivate call urgent at 500-###-####." This is an automated message from (a local credit union)".

Mistry, et. al. suggested the following solutions to smishing [13]:

- Do not call to a given number (received via SMS) which may track your location
- Do not provide any account information to anonymous (untrusted) recipients (via SMS). This is Smishing asking their victims for their bank accounts
- Do not trust any websites or any phone numbers and do not provide them with your account information

V. THE AWARENESS PROGRAM

A. Overview

Although banks protect their online customers from identity theft and financial crimes, the customers should know how to protect their identity information by implementing security best practices when accessing online banking on their personal or business computers. Furthermore, the banks should provide their online customers resources to educate them about best practices for securing their information. Web-based Security Awareness Education (SAE) for bank customer has been implemented in some banks to educate their customers and strengthen the customers' trust to their online banking [18]. Below are our recommendations for awareness of online banking on the following areas: online shopping, online protection, password protection, operating system protection, identity theft protection, and debit/credit cards protection. The purpose of these recommendations is to enhance the customers' trust of online banking and to guide customers into how to safeguard their confidential information from being a victim of identity theft, electronic fraud victim, and other common threats encountered by today's online banking risks.

B. Shopping Online Guidelines

The Internet is the most convenient way to purchase from groceries to houses. The ease and selection that the Internet provides to shoppers has changed the face of retailing. You can go to the retailer's website to make a selection without leaving your chair. When shopping online, we recommend that customers follow the guidelines suggested by Apollo Bank [4]:

- Learn as much as possible about the product and seller
- Understand the retailers' refund policies
- Choose a secure password to protect account information
- Use a secure checkout and payment process
- If an offer sounds highly suspicious or too good to be true, it probably is a scam

C. Best Practices for Online Protection

Several researchers [4, 7, and 17] proposed the best practices for online protection. Here is a list of best practices:

- Reconcile your banking transactions daily and look for unusual small amounts such as penny transactions. This may be an indication that your account has been compromised and a fraudulent plan is in progress
- Never access bank, brokerage, or other financial services information at internet cafes or public libraries. Unauthorized software may have been installed to trap account numbers and log on information leaving the person vulnerable to fraud
- Immediately alert the banks of suspicious transactions. There is a limited recovery window for these transactions and immediate escalation may prevent or minimize further loss
- Do not share your user ID or password with anyone
- Wireless networks are discouraged
- If you use a wireless network, it is suggested that you use password protection
- Always sign out of secure areas of websites, such as Internet banking, where a user ID and password are required
- Be cautious before sharing your email address with questionable websites, as this increases your risk of receiving fraudulent emails
- Delete suspicious emails without opening them; never open attachments in suspicious emails
- When your computer is not in use, shut it down or disconnect from the Internet
- Never provide sensitive account information in response to unsolicited emails, websites, or pop-up windows
- Always review your monthly account statements carefully and investigate any unauthorized activity on your account

- Practice safe internet use. Never click on pop-up messages or links to applications contained in emails. Try to get into the habit of manually going to links that are sent to you. It is estimated that over 80% of malware is obtained from clicking on pop-up ads
- Be suspicious of emails claiming to be from financial institutions, government departments, or other agencies requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes and similar information
- Use caution when opening attachments and ensure they were sent from a trusted source
- Consider designating a "locked down" PC to accommodate only your online banking transactions
- Avoid downloading programs from unknown sources
- Never give out any personal information including user names, passwords, social security number, or date of birth
- Do not use personal information for your user names or passwords, like your social security number or date of birth
- Block cookies on your Web browser. When you surf, hundreds of data points are being collected by the sites you visited. This data get mashed together to form an integral part of your "digital profile," which is then sold without your consent to companies around the world. By blocking cookies, you'll prevent some of the data collection about you
- Do not provide your full birth date on your social-networking profiles. Identity thieves use birth dates as cornerstones of their craft. Try posting only the month and day, and leave off the year
- Use multiple usernames and passwords. Keep your usernames and passwords for social networks, online banking, email, and online shopping all separate
- Online banking customers should be cautious while opening attached pictures via email as it may contain hidden and harmful executable files which will redirect them to the attacker's website
- Online banking customers should not click onto the attached URL via email, but instead they should copy this URL, and paste it into the address bar to be sure that this is a legitimate website

D. Best Practice For Password Protection

The following are some recommendation for password protection [4, 17]:

- Change passwords at least every 90 days
- Create a strong password with at least 10 characters that includes a combination of mixed-case letters, numbers and special characters
- Ensure that your account information and security responses are not written where they can be seen or accessed by others. If the information must be written down, it should be secured under lock and key when not being used
- Never share your user ID or password with anyone for any reason
- Secure your computer with a password-protected screensaver that has a timeout feature activated after no more than 15 minutes
- Avoid using an automatic login feature that saves usernames and passwords for online banking
- Install password management applications to build a strong password, and store it in a secure database instead of putting it anywhere
- Some banks grant their customers a token for accessing their online banking account to enhance the level of security. The user should wait until the code changes and then enter the new code displayed to ensure that the code has not been stolen

E. Best Practices For Operating System Protection

The following are some recommendations for the protection of Operating Systems [4, 17]:

- Ensure that you use a current anti-virus and anti-spyware product to protect yourself against malicious software that is created for the specific purpose of gathering information such as user ID, passwords, and other critical information that may be stored on your computer
- Ensure that you have a patch management solution that keeps your computer software current and can further mitigate new vulnerabilities to which your computer may have been exposed
- Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as DSL or cable. A

firewall limits the potential for unauthorized access to a network and to other computers

F. Best Practice Of Identity Theft Protection

The following are best practices for identity theft protection [4, 17]:

- Report lost or stolen cheques or credit cards immediately
- Never give out any personal information to anyone whose identity you can't verify
- Shred any documents you do not need that contains personal information such as bank statements, unused cheques, deposit slips, credit card statements, pay stubs, medical billings and invoices
- Do not give any of your personal information to any websites that do not use encryption or other secure methods to protect it

G. Best Practice Of Debit/Credit Cards Protection

The following are some recommendation for Debt/Credit Cards protection [4, 17]:

- You should never loan your cards to anyone
- Carry only the cards you use frequently
- Never leave your wallet or purse in your vehicle
- Safeguard your ATM access cards and PIN as you would your cheque, deposit and money. Memorize your PIN – Do not write it on your card or in your cheque book
- Consider using another machine or coming back later if you notice anything suspicious
- When using an ATM, stand squarely in front of the machine to keep your transaction as private as possible
- Consider canceling your transactions if pick-pocketing occurs or any suspicious activities you notice while using the ATM machine
- Protect the sensitive magnetic stripe on the back of your card. Keep it away from direct sunlight. Avoid leaving your card on or near electrical appliances, such as the TV or stereo. Do not carry your card next to another card as they may demagnetize each other
- Report all ATM crime-related activity to the owner/operator of the machine and to local law enforcement officials immediately
- Always take your receipt with you at the conclusion of every transaction to assure your financial privacy. Keep your receipts and use them to check your monthly statements

VI. UAE INTITIATIVE FOR FINIANCIAL PROTECTION

UAE credit bureau was set up and running in early 2014 [19]. The bureau forms a solid partnership with the banks and other financial institutions in the country to ensure the efficient and accurate transfer of information between both sides. The UAE Credit Bureau move intended to [16]:

- Reduce the risk of another wave of bad loans hitting the banking industry, as the one happened in 2008
- Help to reduce borrowing costs for companies and customers with a clean banking record, also it will give the banks more data about the customer's borrowing history
- Support responsible lending
- Enhance payment behavior
- Reduce credit losses from bad or non-performing debits
- Help to strength the UAE's financial infrastructure
- Add demonstrable value to the banking sector

VII. CONCLUSIONS AND FUTURE WORK

The main emphasis of this work is to alert and guide online banking customers to the common security concerns for dealing with the Internet. This is critical because nowadays the Internet has altered people's lifestyles by enabling them from all sorts of life to bring entire libraries, entertainment venues, post-offices and financial centers to the home and workplace. Despite being the most convenient way for shopping, online banking causes significant risks for customers. Attackers and identity thieves are looking to steal online customer's personal information. They target their victim's through their online usage. Although online banks provide their online customers by online security requirements (Terms & Conditions), not all users comply with these requirements. Our goal is to educate customers of the risks of online banking, and how to protect themselves from these risks.

This research opens the door for research questions about the effectiveness of law enforcement responses to victims of online banking. We recommend every online bank to invite their customers into online security awareness conferences and events.

Future direction of this study is to develop a survey and gather data from customers as well as bankers to know their opinion about ISAP. The collected data will be analyzed for the purpose of quantifying the awareness program and to come with further recommendations, if any.

REFERENCES

[1] Abdullah, A. (2014) Protecting your good name: Identity theft and its prevention. Retrieved August 27, 2015, from the World Wide Web: http://dl.acm.org/citation.cfm?id=1059547.

[2] LeClair, J., Abraham, S., & Shih, L. (2014.) An interdisciplinary approach to educating an effective cyber security. Retrieved August 27, 2015, from the World Wide Web: http://dl.acm.org/citation.cfm?id=2528923.

[3] Al-Furiah, S., & AL-Braheem, L. (2014) Comprehensive study on methods of fraud prevention in credit card e-payment. Retrieved August 27, 2015, from the World Wide Web: http://dl.acm.org/citation.cfm?id=1806450.

[4] Apollo Bank's. (2013, 5 2). Customer security awareness program. Retrieved August 27, 2015, from the World Wide Web: http://www.apollobank.com/products/Customer%20Security%20Awareness%20Program.pdf.

[5] Castell, M. (2013, April). Mitigating online account takeovers: The case for education. Retrieved August 27, 2015, from the World Wide Web: https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/130408surveypaper.pdf.

[6] Kalige, E., & Burkey, D. (2012, 12). A case study of euro grabber: how 36 million euros was stolen via malware. Retrieved August 27, 2015, from the World Wide Web: http://www.mtechpro.com/2013/mconnect/february/dyncontent/Eurograbber_White_Paper.pdf.

[7] City State Bank. (2014) Online Banking Customer Awareness and Education Program. Retrieved August 27, 2015, from the World Wide Web: http://www.citysb.com/pdfs/Online_Banking_Customer_Awareness_and_Education_Program.pdf.

[8] Lee Botha, C. (2011, 6). A gap analysis to compare best practice recommendations and legal. Retrieved August 27, 2015, from the World Wide Web: http://uir.unisa.ac.za/bitstream/handle/10500/5457/thesis_botha_c.pdf?sequence=1.

[9] Mannan, M., & P.C. van, O. (2014) Security and usability: The gap in real-world online banking. Retrieved August 27, 2015, from the World Wide Web: https://www.ccsl.carleton.ca/paper-archive/mannan-nspw07.pdf.

[10] Newman, G., & McNally, M. (2007, 7). Identity theft literature review. Retrieved August 27, 2015, from the World Wide Web: https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.

[11] Newman, G., & McNally, M. (2005, 7). Identity theft literature review. Retrieved August 27, 2015, from the World Wide Web: http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.216.6852.

[12] Nilsson, M., Adams, A., & Herd, S. (2014) Building security and trust in online banking. Retrieved August 27, 2015, from the World Wide Web: http://dl.acm.org/citation.cfm?id=1057001.

[13] Mistry, N., Dahiya, M. S., & Sanghvi, H. (2013). Preventive actions to emerging threats in smart. Retrieved August 27, 2015, from the World Wide Web: http://www.ijofcs.org/V08N1-PP03-PREVENTIVE-ACTIONS.pdf.

[14] Peoples Bank. (2014). Online banking customer security awareness. Retrieved August 27, 2015, from the World Wide Web: http://www.ourpeoplesbank.com/Onlinebankingcustomersecurityawareness.htm.

[15] Pipaliya, B. (2014). An empirical study on consumer awareness on internet banking in Gujarat. Retrieved August 27, 2015, from the World Wide Web: http://philica.com/display_article.php?article_id=3 20.

[16] The National. (2014, 1 7). Al Etihad Credit Bureau to allow creditworthiness checks of UAE borrowers. Retrieved August 27, 2015, from the World Wide Web: http://www.thenational.ae/business/industry-insights/finance/al-etihad-credit-bureau-to-allow-creditworthiness-checks-of-uae-borrowers.

[17] Wellington State Bank's (2014). Customer security awareness. Retrieved August 27, 2015, from the World Wide Web: http://www.wellingtonsb.com/14886/mirror/files/Wellington_State_Bank_Customer_Security_Awareness_2013.pdf.

[18] Trustwave. (2014). Security awareness education for banking. Retrieved August 27, 2015, from the World Wide Web: https://ssl.trustwave.com/downloads/sae/SAE.Overview.Banking.pdf.

[19] Al Etihad Credit Bureaue. Retrieved August 27, 2015 from the World Wide Web: https://www.aecb.gov.ae/en-us/services.aspx.

AUTHORS' PROFILE

Khulood Al Zaabi graduated from the University of Sharjah, and has a B.SC in Computer Engineering. Khulood is studying a master degree of Cyber Security at Zayed University, United Arab Emirates. She is working as an IT Security Architect at National Bank of Abu Dhabi. Interested in Cyber Security, Forensics, and Cyber Crime Investigation, Intrusion detection, implementing security awareness's, and conducting a research related Cyber Security and awareness's. Khulood published ISAP: Addressing

Common Security Concerns for Customers in Online Banking at ICT: Big Data, Cloud and Security (ICT-BDCS 2015) conference – Singapore on July 27-28.

Dr. Abdallah Tubaishat is an Associate Professor at the College of Technological Innovation at Zayed University, United Arab Emirates. He received his PhD in Software Engineering from Illinois Institute of Technology, IL, USA. Dr. Tubaishat has twenty years of experience in teaching and research. His research spans two main areas, one is technical: software engineering, and the other is non-technical: e-learning and educational technology. He has published a book with others entitled "Computer Skills", and has around twenty three journal and conference publications. Dr. Tubaishat served on the program and organizing committees of several international conferences and workshops.