THE IMPACT OF ELECTRONIC CRIMES ON THE RISKS OF BANKING FINANCIAL SERVICES IN LIGHT OF THE INCREASING USE OF BANKING INFORMATION TECHNOLOGY AND COMMUNICATIONS

Orooba Rashid Ali AL- Badran, University of Basrah

ABSTRACT

This paper is aims to explain the risks of modern electronic financial and banking services. These services include as credit and debit cards in addition to internet and mobile banking which although had increased Information Communication Technology (ICT henceforth) in finance and banking as well as time, money and effort savings. They created new threats and challenges of cybercrimes including card and email fraud and fishing and hacking. According to the results, cybercrime is reducible in terms of finance by strengthening cybersecurity aspects, improving employee training programs, educating the community, enacting new laws against cybercrime using valid international laws on the basis of relevant information and databases.

Keywords: Financial Banking, Information and Communications Technologies, Cybercrime and Risks.

INTRODUCTION

ICT has revolutionized different human life in various aspects. It made life simpler. It has vaious application such as industries. It has made business simpler by categorising, summarizing, customizing and coding it. The banking and financial services industry is considered as the main industry affected by information technology.

The ICT grew in the financial services adding wealth of opportunities for financial and banking processes enhancing their customers service through adding newer products saving time, money and effort in terms of operation. However, ICT also produces new threats and challenges in the form of cybercrimes.

Cybercrime has become the most dangerous threat to the modern economy; it has affected different sectors including the financial sector. In examining the increasing losses caused by cybercrime, the threats of cybercrime and the measures that should be taken to reduce those threats, this current study focuses on investigating the cybercrime conceptual framework, cybercrime threats on financial and banking services, and cyber threat protection for financial services.

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

Cybercrime Conceptual Framework

Among the many types of illegal acts that affect the average citizen is cybercrime. This phenomenon goes by a number of different names including "crime by keyboard" and "information-technology" or "high- technology" crime.

Definition of cybercrime: It is noteworthy that there is no accepted definition for cybercrime worldwide. International Organization of Securities (IOSCO) Research Department refers to cybercrime as a negative activity which a group can cause (for example two groups of grassroots nationally coordinated groups) by computers; it could also include the IT systems and/or the internet attacking computers, IT infrastructure and internet when there is one more entity. It is the use of computer or other electronic devices via information systems to facilitate illegal behaviours (Gercke, 2017).

The United Nations in its tenth congress on "prevention of crime and treatment of offenders" related crimes of computer networks. Cybercrime has two main types:

Cybercrime in its narrower term is called computer crime. It is any illegal activity achieved electronically targeting the computer system security and its data.

In its broader sense cybercrime is called computer-related crime. It is an illegal activity that is linked with computer system or network, for example, in which crimes can mean information possession and distribution illegally (Singh Poonia, 2019).

Reasons for Cybercrime

Computers could be vulnerable due to (4):

Comparatively small space capacity of data storing: Computer can store data in small spaces supporting the removal or derivation of information by physical or virtual medium esily.

Easy access: Protecting a computer system from unauthorised access faces many possible breaches not because of human errors but because of the complexity of technology. There are different ways fooling biometric systems and bypass firewalls, to access the security system such as the secret implantation of logic bomb, key loggers stealing access codes, developed voice recorders and retina imagers.

Complex: The operating system computers work and their operations consist of millions of codes. Humans make mistakes at any phase possibly. The cyber criminals exploit these mistakes and illegally access the computer systems.

Negligence: This aspect is in a very close link to human activity making it possible when protecting the computer system. This in turn adds a cybercriminal access and control over the system of the computer.

Loss of evidence: Evidences can be lost because most of the data are usually destroyed. Additional data collection outside the territory also paralyses this system when a crime is investigated.

Classification of Cybercrime

There are many types of cybercrime prevailing in the system; broadly, we can classify them into four major categories as discussed below (Dashora, 2016) (Net Losses, 2019).

Crime against individuals: Cybercrimes committed against individual persons include crimes such as transmission of child pornography, harassment towards people with the use of a computer such as via e-mails, hacking, indecent exposure, e-mail spoofing, cyber defamation, IRC crime (Internet Relay Chat), malicious code, net extortion, distribution, postingcredit card

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

fraud, phishing, trafficking, and obscene material dissemination such as software piracy. The potential harm that such crimes can do to a person can be massive.

Crime against properties: Another classification is cybercrimes against all forms of properties. These crimes include computer vandalism (obliteration of others' property), intellectual property crimes, threats, and salami attacks. Crimes of these kinds are common in financial institutions. Its significant feature is that amending it is so small which would not normally be observed.

Crime against organizations: This type of crime relates to cybercrimes against organizations. Cyber Terrorism is one discrete type of organizational-based cybercrime. The advances of the Internet help showing the standard of cyberspace individuals' and groups' use for forcing international governments and intimidate people. This crime evolves into terrorism when the attacker "cracks" into a government or military websites. There is unanimous a universal acknowledgement that each and every system in the world is subject to crack.

Crime against societies: The fourth classification relates to cybercrimes against societies such as cyber terrorism, forgery and jacking of web. They could destroy the youth by indecent exposures, data diddling, illegal article sales, financial crimes, cyber contraband, net extortion, logic bombs and salami attacks. Notes of currency, stamps of revenue, sheets of mark etc. are subject to forge through computers and advanced printers and scanners. Hackers of web jacking could access and control others' website and change the website content to fulfil their political or financial objectives

.

Effects of Cybercrimes on the Global Economy

In the past, cybercrimes were committed mainly by individuals or small groups; today, cybercrime is a rampant misconduct. Several criminals exploit the speed. Convenience and the Internet anonymity are exploitable to commit different criminal activities with no physical or virtual limits causing serious problems and serious threats to victims universally. Cybercrime has many effects on the global economy.

Potential Economic Impact

The Centre for Strategic and International Studies (CSIS) sponsored by McAfee reported that Cybercrime businesses could cost about US$400 billion universally impacting about 200,000 and 150,000 jobs in the US and n the EU respectively (6). The trade of cybercrime, competitiveness, global economic growth and innovation. About the Internet annually creates about $2 to $3 trillion, a share of the global economy growing rapidly. The CSIS estimates this crime extraction ranges from 15% to 20% by the Internet. Cybercrime's impact on intellectual features is in particular damaging. It progresses as the intellectual property creation and -intensive industries to create wealth lose in trade, income from cybercrime jobs than countries with low-level manufacturing agriculture or industries.

Impact of Cyber Crime on Consumer Behaviour

There is a link between the information revolution and the strategic Internet leveraging which make the societies relatively open to cybercriminal and cyber terrorist activity. This is in particular in transactions of commercial business. In developing e-commerce, this commercial

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

dark side, cybercrime, has taken many forms affecting online shopping. Firms must understand these threats to their online businesses with strategic implications on their prospective businesses. Thus, proper measures must be taken for ensuring the elimination of threats so confidence of consumer in the Internet is seen as an alternative to shopping (Das and Nayak, 2018) .

Impact on Market Value

The financial effect of security breaks is of intrigued to firms that are attempting to choose where to put their data security budget as well as for protections companies that give cyber-risk arrangements. This unused and advancing see of harm gets to be indeed more vital as numerous firms depend on data frameworks in common and the Web in specific to conduct their commerce. This point of reference may drive numerous protection firms for the compensation of businesses for harm because of the programmer assaults and other security flaws (Saini & Shankar Rao, 2017).

Threats of cybercrime in financial and banking services: The information-driven society growth has given openings for budgetary keeping money teach to upgrade administrations to clients through modern items making differences to spare time, cash and exertion from in terms of operation. Yet, the inverse conclusion and cybercriminals show better approaches to shortcomings and working for the generation of more modern strategies of assault. Or, they find high-tech rehashes of ancient traps that taken a toll customers and the society entirely.

The Most Important E-Financial and Banking Services Targeted By Cybercriminals

The integration of ICT and financial services has generated many new electronic services that led to an increase in cybercrime activities. But the most important e-financial and banking services that are targeted by cybercriminals are:

Payment cards (9): This type of carda is regularly a 3 ⅜" by 2 ⅛" plastic. It has a magnetic stripe or a computer chip to store the user's information. It counts card number and termination date. This card and incorporates credit, charge, and paid in advance cards.

Credit Card: A credit card is any card useable for borrowing money or buying services. The balance payable in full in a deadline or paid over time with interest when the borrower forces minimum payments on a month basis in amounts set by the card-issuing bank with a retail, store and other businesses issue.

Debit Card: There is a link between this card and a checking or other deposit account in which funds are drawn for settling debit card transactions including a sale or purchases or ATM withdrawals. Cardholders sign their name or entering a personal identification number to authorize debit card transactions by (PIN).

Prepaid Card differ from credit and debit cards in their offer of paying early for prospective purchases for their consumers. The money is prepaid into the card account. Also, these funds can be used later through the presentation of the card to pay at accepting merchants or, by a card with a PIN for withdrawing cash at ATMs.

Online banking: This type of banking enables bank clients to access their accounts and common data on bank items and administrations. It is also easy with this type of banking to perform account exchanges with the bank through an individual computer by the use of the Web

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

as the conveyance channel; clients are able to get to all of their accounts in the site of the bank and are permitted to conduct managing an account exercises such as exchanging stores, paying bills, seeing account equalizations, paying contracts or obtaining budgetary rebellious and certificates of deposits (Drigas & Isac, 2019).

Mobile banking: A bank account is an application of portable computing which gives clients the bolster required to bank anyplace, regardless of time employing a portable handheld gadget and a versatile benefit such as Brief Message Benefit (SMS). Banking money offices evacuate the space and time impediments from managing an account including checking account equalizations or exchanging cash from one account to another. It saves time from reaching to the bank to perform managing account exchanges.

Threats Faced by the Financial Services Sector

The threats of the financial service industry faces are larger than those of other industries, nine of which are.

Advanced persistent threats: APTs utilize undetected, persistent computer hacking forms to access all esteem organization's Network. Phishing emails and/or other traps are used for tricking representatives into downloading malware. This is a common problem. When there are unauthorized individual accesses, they frequently go unobserved for a long period of time. This happens in a quiet manner to take information, commit extortion, crush an institution's financial soundness or undermine its notoriety

Insider and internal threats: The company can be harmed by authorized employees, contractors, supplier, or business partners with an uncontrolled access to systems. They may also have access to sensitive information with possible irrevocable harm. This has increased substantially with the increased of personal devices, and e-mails, and USB storage and cloud-based. One purpose or not, insiders can ruin the systems. They can also open them to malicious intrusion, and steal, make fraud, or manipulate market.

Denial of service attacks: This type of threats is "any attack intended to compromise the availability of networks and systems". They are concerns to financial institutions using trading systems on websites. These attacks target networks with phony linking requests that make it prevent the processing of legitimate application.

Account takeovers: Cyber offenders have rapidly found how to abuse budgetary and showcase frameworks that interface with the Web, including the Automated Clearing House (ACH) frameworks, card payment, and showcase exchanges. Abusing framework clients, instead of the frameworks themselves, win offenders get to bank or credit card accounts or budgetary frameworks, and permit carrying out unauthorized exchanges. A recent report on cybersecurity within the managing an account segment distinguished that nearly half (46%) of the educate detailed account control as the foremost visit cyber interruption movement they experience.

Breaches of securities and market trading: Cyber criminals target the securities and brokerage business, ffinancial institutions and customers commonly. In some studies, markets are commonly manipulated and there is an unauthorized stock trading risks which traders and their exchanges face.

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

Third-party-payment processor breaches: Complex cyber criminals target computer networks with large payments that result in wasting millions of dollars and the personal information compromising millions of individuals.

Supply chain infiltration: In later a long time, cyber hoodlums focused on trusted providers of specialized, computer and security gear, program and equipment that aim to pick up physical and specialized access to banks. Cyber offenders are ceaselessly concocting better approaches to penetrate money related educate, from posturing as seller representatives to conveying contaminated gear. A few later assaults included equipment introduced in bank department frameworks to empower exchanges to be controlled by means of versatile systems.

Mobile banking breaches: Meeting customer demands for better mobile banking capability has made financial institutions susceptible to other cyber threats. Cyber criminals are very quick in understanding the way of exploiting the susceptibilities in mobile technology. This is through the use malicious websites, text messages, or mobile applications which help gaining access to a user's credentials and account information.

Payment card skimming: A skimmer fitted to the exterior or interior of an ATM or gas station pumps empowers criminals to gather card numbers and individual recognizable proof number (Stick) codes. The stolen information is usually sold or utilized to create fake cards to withdraw cash. As firms proceed to roll out and shoppers embrace new electronic, remote instalment frameworks, hoodlums are rapidly adjusting. Programmers have as of now outlined Bluetooth-enabled remote skimmers to right away download information when in run of the remote arrange.

Impact of Cybercrime on Financial Services

Before analysing the impact of cybercrime on financial services, we must first know the types of cybercrimes.

Types of cybercrimes in the financial sector

There are various types of cybercrime in financial services, such as the ones we have just mentioned. They may include:

Credit card fraud: When credit card or debit card is used by costumers for any online payment, several credit card frauds are made when a person acts with mala fide intent to use these cards (Singh et al., 2016).

E-mail fraud: Today, e-mails and websites have become the preferred means of communication due to their speed and ease of use. Hackers will send emails to bank customers stating that they have won something and that in order to claim the prize they would have to share their bank details. Gullible customers would simply give out their banking information which the hacker can then exploit for their own benefit.

Phishing: This entails the attainment of information including usernames, details of credit card or passwords and so on by electronic communication. Phishing commonly involves the usage of fake e-mails or fake messages which contain links to websites that are infected with virus/malware. These websites request users to enter their personal details.

Hacking: This entails an illegal access to a system to gain information in terms of both the operation and its data, which are then adapted to fir the hacker's needs and the word 'hacking' has both negative and positive connotations (15).

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

Effects of cybercrime on financial services: Financial services organisations have suffered from various economic crimes. Based on the reports of the PricewaterhouseCoopers Global Economic Crime Survey in 2019, cybercrime is one of economic crime, which are very common. This is what the financial services respondents reported in 2016 and 2019 as 38 percent 39 respectively (Figure 1).

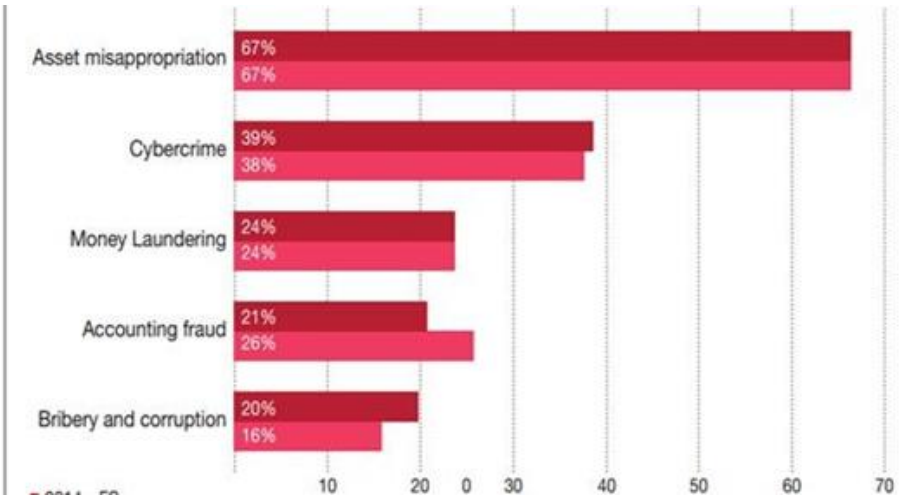

FIGURE 1
TOP 5 TYPES OF ECONOMIC CRIME EXPERIENCED BY THE FINANCIAL SECTOR DURING THE SURVEY PERIOD

By taking advantage on the many facilities provided by the financial sector like Internet banking, credit card facilities, debit card facilities and online transfer, cyber-attacks targeting financial services firms are on the rise.

According to a Kaspersky Lab, 93% of financial service organizations have experienced various cyber threats in the past 12 months. This has caused an average annual loss of 28.33 million US dollars in financial sectors in the US. Meanwhile, cybercrimes in the United Kingdom has caused a loss of 2.4 million pounds, and 46.4 billion in China.

Cybercriminals have committed worldwide frauds on credit cards and debit cards in addition to the prepaid cards. They reached $16.31 billion last year on total card sales volume of $28.844 trillion. This is mainly because many people who do not understand technology well are using credit and debit, POS, ATM, online and mobile banking facilities without proper security measures. Cybercriminals with mala fide intention take advantage of such vulnerabilities for their own benefit.

Kaspersky Lab products shows that the detected and neutralized reached 6,167,233,068 threats in the reported period in which the Kaspersky Lab solutions blocked 1,910,520 attacks for launching malwares. These malwares are able to steal money from online banking accounts and 12,100 mobile banking Trojans (Figure 2).

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

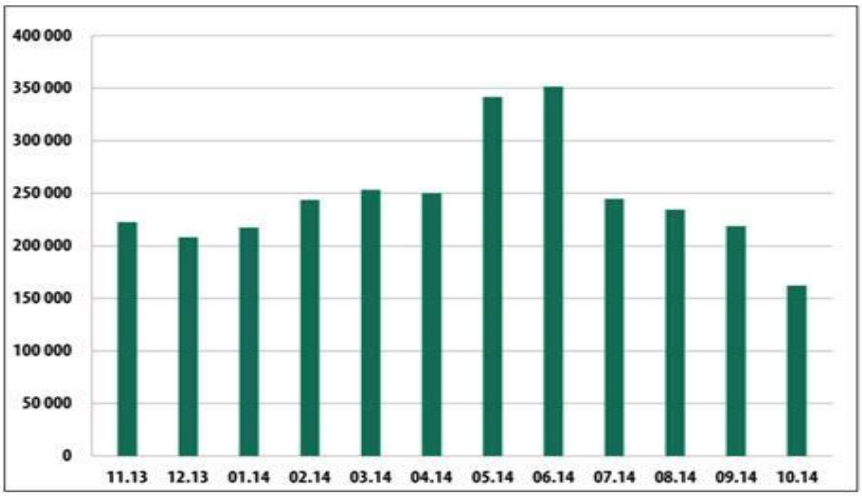

FIGURE 2
ONLINE THREAT IN THE BANKING SECTOR

Cyber Threat Protection for Financial Services

To protect financial services from the risks of cybercrime, these procedures can be taken:

Procedures related to the strength of cybersecurity: Technology crimes are one of the strong attacks on technology itself. Yet, different practices have been taken in the majority of the financial services firms to protect from the types of. However, to getting ahead of the threats need developing information security abilities to excel operation. It requires (17):

Advanced authentication: Advanced authentication offers a more improved protection practice than that of the traditional security and anti-fraud approaches. It is individualised for each user resulting in resisting the industrial-style automation which is a feature of mass attacks. It is not just an identity management, but also an advanced authentication methodology that monitor users' features and behaviours. It prevents imposters from accessing infrastructure and data. The features can be the users' normal locations, applications, devices and configurations. The behaviours are users' typical access day, path through the site and recent browsing history.

Advanced automation: The automation of the security response and mitigation processes make progress so slowly that it remains behind monitoring and alerting. The combination of human intelligence and log data into a delicate threat detection and discrimination system makes an automated response. For instance, when a bad actor is identified by any other security controls such as IP, URL, an automated solution only blocks the activity and send an alert, but also separate the affected part from the network. In addition, it takes an image of the system for forensics. This is supported by improving it and bringing back online.

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

Big Data analytics/security intelligence: Financial companies collect different security information volumes such as endpoint and network device logs, user data and asset. The engines of the rules-based and algorithms of machine-learning accelerate the modern data-mining and visualization techniques. These techniques could be able to identify high-risk outliers with sensitivity which is not known yet. Traditional labour-intensive process and cybercrime analysis will increase the leverage Big Data use. This, it improves the structured and unstructured use of powerful, real-time analytics across multiple data sets. It in turn in improves the analysis of real-time cyber threat in terms of quality and speed when it significantly reduces the overall expenditure.

Procedures Relating to Personnel

The improvement of the employee training program by means of comprehensive user-awareness program could assist the organizations in improving their security culture. This is by the establishment of a baseline of current risky behaviour by using simulated phishing testing and individual responsibility training employees and measuring developments.

Procedures Relating to Community Education

In general, the community needs to be educated. In particular, this applied to the group with the end user of computer and network systems. This subset is usually he direct victims of cybercrime and finally indirect victims in the extra payment while the companies they support are also victims and forced to spend extra taxpayer dollars annually as an answer to the computer-related crimes. IT professionals and Law enforcement are required to cooperate with the community for building a cyber-fighting team with the skills and the authority required for a great reduction of the Internet crimes instances.

Procedures Relating to Legal Systems

The delay in the possible abuses of recognition of new technologies and main modifications is one of the obstacles to the national criminal law and the legal system. These obstacles are still relevant. In addition, they are also topical as the speed of the acceleration of the network innovation:

1. Adjusting the national law to recognize the new technology abuse.
2. Identifying gaps in the penal code ensuring the valid legislative foundations.
3. Drafting of new legislation.

Although many countries have enacted new laws fighting cybercrime starting with the United States of America in 1978 and expanding to most countries including Arab countries such as Saudi Arabia and the United Arab Emirates, they are incompatible with local character and contain legal gaps. Therefore, it is necessary to establish effective international laws according to the information and databases of graphic information specific to this aspect.

CONCLUSION

The benefits of technology such as scale, speed and low error rate reflect the performance, productivity and profitability of financial services, which have improved tremendously in the

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.

past decade. Technology-related initiatives have been undertaken by financial institutions in the areas of mobile banking, electronic payments, and the Internet, but they have also enabled the occurrence of cybercrimes.

Cybercrime i.e. the illegal activity conducted by, or related to, a network or system of the computer. These crimes include, for example, mala fides or distribution of information by a computer or a network, is the second most commonly reported economic crime in the financial services sector, accounting for 38% of incidents. Cybercrime expenditure in businesses is about US$400 billion universally, affecting about 200,000 150,000 jobs in the US and the European Union, respectively. This is via card frauds, fishing, e-mail fraud and hacking.

The fight against threats of cybercrime entails four procedures. The first is related to the strength of the cybersecurity which involves advanced authentication, advanced automation and big data analytics. The second procedure is related to the personnel i.e. by strengthening employee training programs with comprehensive user-awareness programs. The third procedure is related to community education i.e. by educating the community at large, especially the subset that consists of the end users of computer and network systems. The final procedure is related to the legal aspect i.e. by making adjustments to national laws with the identification of the penal code gaps. This procedure also aims to draft new legislations for valid universal international laws on the basis of relevant information and databases.

REFERENCES

Cyber Security for Financial Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust, Symantec White Paper, 2015, p 07. (18)-Mohamed CHAWKI, A Critical Look at the Regulation of Cybercrime, at: www.crime-research.org (visited 31/03/2016).

Dashora, K. (2016). Cybercrime in the society: Problems and preventions, rural of Alternative perspectives in the social sciences. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.452.5880&rep=rep1&type=pdf

Das, S., & Nayak, T. (2018). Impact of cybercrime: issues and challenges, International *Journal of Engineering Sciences & Emerging Technologies*, 149.

Drigas, I., & Isac, C. (2019). E-banking services features, challenges and benefits. *Annals of the University of Petroşani, Economics, 14*(1), 53.

Federal Reserve of Philadelphia, what you need to know about payment cards. Retrieved from https://www.philadelphiafed.org/

Gupta, V.K., Begonia, R., & Bagoria, N. (2018). Mobile banking services as adoption and challenges. *International Journal of Scientific and Research Publications*, *3*(1), 1.

Gercke, M. (2017). Understanding cybercrime, phenomena, challenges and legal response. ITU. Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Kandpal, V., & Singh, R.K. (2018). Latest face of cybercrime and its prevention in India. *International Journal of Basic and Applied Sciences, 2*(4), 151-152.

Net Losses: Estimating the Global Cost of Cybercrime. Centre for Strategic and International Studies, June 2019. Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf

Saini, H., & Yerra Shankar Rao, T.C. (2017). Panda, Cyber-crimes and their impacts: A review. *International Journal of Engineering Research*, 205.

Singh, D., Rathore, H., & Marwah, K. (2016). Cybercrime in banking sector, international journal Law mantra,Journal.lawmantra.co.in www.lawmantra.co.in. (visited 28/03/2016.

Singh Poonia, A. (2019). Cyber Crime: Challenges and its Classification. *International Journal of Emerging Trends & Technology in Computer Science, 3*(6), 120.

Singh Poonia, A. (2019). Cybercrime: Challenges and its classification. *International Journal of Emerging Trends & Technology in Computer Science, 3*(6), 120.

Citation Information: Ali AL- Badran, O.R. (2021). The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal, 27*(6), 1-9.