Aftab *et al.LGU (IJECI)* 2022

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 6 issue 4 Year 2022

Frauds in Banking and Entrepreneurs by Electronic Devices and Combating Using Software and Employment of Demilitrized Zone in the Networks

Prof. Dr. Aftab Ahamd Malik[1], Dr. Mujtaba Asad[2] and Dr. Waqar Azeem[3]

[1]University of Kent, England.

[1] Department of Criminology and forensic Sciences, Lahore Garrison University, Lahore

[2]Shanghai Jiao Tong University, China

[3] South Eastern Regional College, Downpatrick, Ireland UK

Corresponding author: dr_aftab_malik@yahoo.com

Abstract

The malpractices and frauds are exponentially rising in developed and developing countries in the entrepreneurs, banking as well as medium sized companies. The criminals are utilizing most modern information technology structures and such electronic media to accomplish their offence regarding fraud to cause wrongful loss and harm in the areas of white collar crimes, banking, business and to individuals. The purpose of this research paper is make these companies realize the essence of using most recent, most reliable and most authentic software and need to make their networks more secure from outside attacks. The use of advanced features of tracking and hacking confidential information using information technology resources enables the criminals to achieve their objectives. Basically, their modes operandii depend upon dishonesty and deception to complete the offence. In the banking and white collar frauds most of the time the employees of the concerned organizations are involved, who help and collaborate external criminals by passing confidential information. The fraud is constituted by parody, distortion, misrepresentation and twisting the fact/truth or concealment of a real information detrimental to someone else. The legislation seems very naïve to punish the criminal who have committed frauds. There are several reasons for the criminals to escape, for example their identity is most of the times remains hidden. Lack of evidence, feeble investigation and naïve role of prosecution in the court of law enables the criminals to go towards exoneration and release. The paper also presents analysis of various types of frauds existing in the society and how to combat with them effectively. The main objective of the fraudsters is to deprive people or entrepreneurs of their money, property, valuable documents and private information. The authors of this paper express their deep concern on taking strict measures to safeguard the rights of bank customers by introducing most recent software versions and the government must introduce stern and stringent legislation in this direction.

Keywords: Demilitarized zone (DMZ), Fraud, Hacking, Financial Crimes, Cyber Crime

1. Introduction

According to [1] the corruption purchasing and selling of securities from the period 1870 to 1940 and [2] from 1940 to 1980 is discussed in depth; while [3] highlights the history of frauds in American Business and designing of self-regulations related to the period 1895 to 1932. According to [4] and [5] frauds in the American history have been discussed and [6[emphasizes on understanding the legal procedures, plan, policy and practice. The behavior in case of committing frauds involves the ingredients such as apparent, superficial financial need and reasoning for validation and its rationalization. Legally speaking, the fraud is constituted in the court as a state of affairs where by misrepresentation occurs to act upon the fraudulent behavior. It is an act with criminal obligation for fraud to gain money or "services" with dishonest intention. Deception, illegal gain, opportunity and motive are essential constituents of frauds.

Figure 1: The Fraud Triangle hypothesizes [Reference: Fraud Examiners Manual]

There is another large Money crime Fraud reported in [8] regarding loans and savings crisis. The assertions of the authors are based on 100 interviews and several documents on the subject matter of this big-money criminals. This case may be termed as worst fraud of the twentieth century happed in 1980. Inclusive of the interest, the fraud amount is estimated to be US $ 175 billion. This fraud involves a chain of white collar crimes, not found in United States of America. The famous financial specialists have discussed this fraud and the authors of [8] are of the opinion that this fraud is as "systematic political collusion" due to the presence of political involvement. In this case notorious offender was as central criminal named Charles Keating. The performance of law enforcement agencies had not been adequate. According to vision of [9], there is tremendous scope of research in the area of frauds particularly in accounting, society, organizations and public private sector autonomous and semi-autonomous bodies.

2. Vision of British Law on Frauds

The legislation promulgated in UK reported in [7] is called the Fraud Act 2006. Its sections (1),(3),(4),(5) and (12) are important for discussions on the topic of this paper. Section 1, deals with breaching the law by misrepresentation implicitly or explicitly; while Section (3) discusses the frauds and to cause harm to others by failing to reveal information and the Section (4) relates to fraud by misuse, exploitation and abusing the position of the offender by omission or commission of offence. In Section (5) it is termed by fraud as permanent or temporary "gain" and "loss" in terms of money, things or imperceptible or incorporeal property, which is distinguished. According to Section (12), the frauds commit-

ted by the officers of an entrepreneur is regarded as Obligation, Accountability and Liability of the entrepreneur or company or corporate body concerned. Section (13) provides all the necessary legal aspects regarding the question of " Evidence", which an enquiry officer must keep in mind because the entire case of prosecution depends upon the collection of strong evidence during enquiry. The offender must not be excused on issues of not answering any question regarding the property, accounts of property and relevant documents. If there exists any conspiracy in fraud, it must also be highlighted and reported in the enquiry.

3. The Frauds committed using Internet

The fraudsters involved in the frauds utilize modern software tools and programs, coupled with internet connection to access the information, particularly the Email of the victim and other identity features. The frauds committed on internet therefore are called Email-based or online cybercrime. The fraudsters are interested to hack identity to further commit other cybercrimes and defraud victims of their money. In this way millions of dollars of frauds are carried out by dint of internet scams using online facilities. The number of frauds on internet is exponentially increasing with design of new techniques.

Cybercriminals possess advanced information technologies, which are coupled with internet to carry out offences. Mostly they initiate their offence from having personal information and identity of their victims. They commence a series of attacks using different schemes and algorithms and messaging services to capture user's data. There are several groups and types of internet attacks such as Business email compromise (BEC), spoofing and Phishing, Ransomware, Lottery Fee Fraud, Credit Card Scams, Online Dating Scams. In 2020, 95% of all attacks on company networks were spear phishing-related, and 22% of all data breaches included a phishing attack, according to research from Security Boulevard. Additionally, about 2 million new phishing websites are launched, 97% of users cannot identify a sophisticated phishing email, and 78% of users are aware that clicking links in emails can be dangerous. Email-based phishing scams are always evolving, ranging from simple attacks to sophisticated threats that specifically target certain individuals.

3.1 Cyber Crimes

In Pakistan people keep them busy on internet in the areas of social networking, audio and video exchange, and do online shopping and online banking transactions. During Covid epidemic the academic institution held online classes and examinations. The Cyber Crimes are carried out using computer or other digital devices and networks. The spread of different viruses, sending messages of insult and to harm the users, the criminal trespass their accounts and networks, especially they take away heavy amounts of money from the banks using illegally acquired information. Apart from other offences, one of the occupations of such criminal is also drug trafficking. The can hack the data from any network within 3 to 4 seconds with recent softwares. The digital piracy and electronic terrorism are also serious areas of cybercrime to combat.

4. Internet Frauds and Protective Measures

The user's may adopt adequate measures to protect their useful and private information to avoid the outside attacks. Users also must use powerful anti-spam. Computer fraud is closely related to online fraud, is described as using a computer or computer system to facilitate the execution of a scheme or illegal conduct and aiming a computer with the intention to modify, harm, or disable it. While not working with internet, one muss switch off Wi-Fi Network as well as Wi-Fi routers.

Table 1: Protective measures

SR #	Measures to avoid internet frauds
1.	While not working with internet switch of Wifi
2.	Be watchful and cautious to avoid being caught in a phishing
3.	Must have knowledge of common internet Frauds and modus operanii of hackers
4.	Never send money to anyone who is acquainted to you on internet
5.	Keep your personal and identity information strictly confidential to others, especially unknowns
6.	Avoid clicking on attachments or hyperlinks in the messages received from Emails
7.	In case of any attacks from hackers report to the concerned authority of Email.
8.	Keep on Checking frequently yor bank accounts to avoid fro Credit card frauds.
9.	If Credit Card Fraud occurs, immediately report to to Bank legal authorities

5. Financial Frauds in Pakistan

Nowadays, almost all banks are providing their customers the facility of online banking to open accounts, payments of utility bills, online payment taxes, credit and debit cards, processing of the loan applications and having bank statement online. These facilities sometimes involve technical and operational errors and mistakes. Most of fraudsters aim at depriving the victims of their money. The financial frauds involve, Phishing. Card skimming, prize Bonds, false Lottery Schemes, frauds though online payment networks, though, Imitating, Copying and Impersonating organizations and banks. The initiation of fraud begins from obtaining personal information and Identity theft of the victim. The malpractices in credit and debit card are exceeding at very high limit in Pakistan. Another type of frequent fraud occurs in the field of loans and property mortgage, falsehood in employment, online collection of advance fees.

In banking applications, most of the complaints logged by customers are due to corrupt practice s of bank employees and officers, delaying tactics to handle the customer's grievances, criticisms and complaints. Sometimes the banks do not strictly act upon the policy and instructions of the State Bank. The banks must adopt most recent development in banking to deal with banking-business using new information technologies and protective measures to combat the frauds at large scale. The Bank customers may lodge their complaints regarding unresolved complaints and issues with banks to "Mohtasib Pakistan". The usual modus operandi in Frauds related to banking is accomplished by mafias of fraudsters is that firstly they call the consumers misrepresenting as bank personnel

and representatives to cheat, betray and deceive the customer to get the financial information. Then this information is used to harm the consumer in the fraudulent offence, consequential in financial loss. In 2022, the federal Government of Pakistan decided to compensate a relief of Rs 1.9 Million to account holders facing frauds, particularly to victims ordering Bank Alfalah Ltd (BAL) to refund the defrauded money. For the consumers, the State Banks of Pakistan issues fraud warnings from time to time therefore, the consumer must look into the guidelines. "In a recent warning to the general public, the State Bank has told that name "State Bank", its official and authorized logo is used by the fraudsters for deceitful purposes and determinations. Then the victim is communicated of cash to be paid by way of inheritance by the State Bank's Overseas Branch." Therefore, the victims are asked to give personal information such as identity, mobile numbers to have access to their funds in banks, particularly in case of overseas.

The study presented in [12] discusses the involvement of bank employees and they pledge and commit various types of frauds to harm the victims. The researchers have proposed several measures in this regard. The most important is that individual banks must also take positive initiatives to minimize and control the harm caused to the bank and hence the innocent victims. The reader may consult the research contents and results from [12].

In this section very briefly the usefulness of Demilitarization Zone (DMZ) is mentioned which is used to secure the Network (LAN) from the hackers and trackers. It must be employed in all the public and private organizations using Network (LAN). According to [14], applying DMZ ensures in refining the network security of web testing.

Table 2: Statistics

Region	Complaints received during the year	Complaints Carried forward from last year	Total
Punjab	20885	2625	23510
Sindh	7614	1062	8676
Khyber Pakhtunkhwa	3028	421	3449
Balochistan	552	44	596
Gilgit Baltistan	63	3	66
Azad Kashmir	246	0	246
Overseas	808	13	821
Total	**33196**	**4168**	**37364**

A DMZ configuration in a Local Area Network allows additional defense mechanism against external attacks to (LAN). A DMZ is a physical or logical subnet that separates a LAN from untrusted networks, such as the public internet. Any service offered to open internet users should install the DMZ. The systems that run

services on a DMZ server are susceptible to attack by hackers and online criminals. For those servers to be able to withstand ongoing attacks, security must be enhanced. The purpose of the DMZ network is to safeguard the host's data and work.

DMZ networks are implemented to safeguard critical resources and systems. The DMZ is often shielded from access to everything on the external network by a second firewall. Most of the time, internal assaults like spoofing via email or other methods or sniffing communication with a packet analyzer are unaffected by the greater security given by external attacks.

Organizations no longer require internal web servers, thanks to cloud computing. Network security for both individual users and large companies depends on DMZs. By prohibiting external access to internal servers and data, which can be seriously compromised, they securely protect the computer network. Before incoming network packets reach the servers, a firewall or other security tools can monitor them; thanks to the DMZ firewall configuration.

7. Design and Structure of the DMZ

A DMZ can be used to build a network in a variety of ways. A single firewall (also known as a three-legged architecture) or twin firewalls are the two main strategies for accomplishing this. Both of these technologies can be developed further to create intricate DMZ designs that meets network needs.

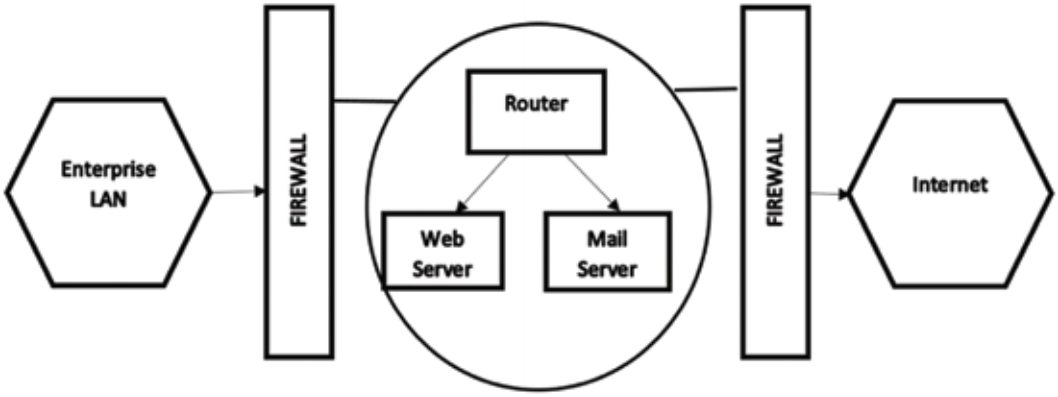

Figure 2: Architecture of Demilitarize zone in a Computer network (LAN)

8. Advantages of DMZ

A DMZ can be used to build a network in a variety of ways. A single firewall (also known as a three-legged architecture) or twin firewalls are the two main strategies for achieving this. Both of these technologies can be developed further to create complex DMZ designs that meet network needs. The DMZ guards against efforts to spoof an IP address in order to gain access to systems. Such attempts can be detect-

ed and stopped by a DMZ while another service verifies

9. Recommendations

a. Protective measure for Cyber Crime,

b. Face Book must be secured,

c. Take essential security measures such as Login alert and security code,

d. Permit to your restricted friends to view your videos and pictures,

e. Login notification must be adhered to and used,

f. Also limit your contacts,

g. Disable your debit/credit card as soon as possible if you lose them,

h. Adopt a secure way to communicate your Cash Transfers,

i. The banks must adopt most recent developments in banking to deal with banking-business using new information technologies and protective measures to combat the frauds,

j. For online Shopping, the customer must choose the mode of payment by cash on receipt of the parcel.

k. For the consumers, the State Banks of Pakistan issues fraud warning from time to time therefore, the consumer must look into the guidelines. Therefore, follow up the guidelines in accordance with reference [11]. Further, ignore any incoming message from State Bank as a result of fraudulent misrepresentation of fraudsters

l. The Bank customers may lodge their complaints regarding unresolved complaints and issues with banks, to the "Mohtasib Pakistan".

m. In case of security and problem related to cybercrime, Cyber Crime Prevention, Federal investigation agency, National response center for cybercrime: https://nr3c.gov.pk/cybercrime.html

n. May also contact, National Police Foundation Building, Mauve Area Second Floor, Sector G-10/4, Islamabad, Pakistan. Phone: +92 51 9106 384; Email: helpdesk@nr3c.gov.pk.

10. Acknowledgement

The authors are deeply indebted to Mr. Kaukab Jamal Zuberi Head, Department of Criminology and Forensic Sciences Lahore Garrison University for guidance and Dr. Syeda Mona Hassan Chief Editor of the Journal for encouragements.

11. References

1. Armstrong, C . (1997). Blue skies and boiler rooms: Buying and selling securities in Canada, 1870– 1940. Toronto: University of Toronto Press.

2. Armstrong, C . (2001). Moose pastures and mergers: the Ontario Securities

Commission and the regulation of share markets in Canada, 1940-1980. Toronto: University of Toronto Press.

3. Balleisen, E. J . (2009). Private cops on the fraud beat: The limits of American business self-regulation, 1895-1932. Business History Review, 83 , 113–160.

4. Balleisen, E. J . (2017). Fraud. An American history from Barnum to Madoff. Princeton: Princeton University Press.

5. Berghoff, H . (2018). “Organized irresponsibility”? The Siemens corruption scandal of the 1990s and 2000s. Business History, 60 , 423–445.

6. Baldwin, R. , Cave, M. , & Lodge, M . (2012). Understanding regulation: Theory, strategy and practice (2nd ed.). Oxford: Oxford University Press.

7. Fraud Act 2006 - Legislation.gov.uk; https://www.legislation.gov.uk

8. Calavita, K, Pontell, H. N, & Tillman, R. H. (1997). Big money crime: Fraud and politics in the savings and loan crisis. Berkeley, CA: University of California Press.

9. Cooper, D. J. , Dacin, T. , & Palmer, D . (2013). Fraud in accounting, organizations and society: Extending the boundaries of research. Accounting, Organizations and Society, 38 , 440–457.

10. Cyber Crime Prevention, Federal investigation agency, National response center for cybercrime: https://nr3c.gov.pk/cybercrime.html

11. Fraud Warning - State Bank of Pakistan, https://www.sbp.org.pk › pdf › PublicWarning-01

12. Younus, M. (2021), "The rising trend of fraud and forgery in Pakistan’s banking industry and precautions taken against", Qualitative Research in Financial Markets, Vol. 13 No. 2, pp. 215-225. https://doi.org/10.1108/QRFM-03-2019-0037. 242-0905.

13. Hugo van Driel (2019) Financial fraud, scandals, and regulation: A conceptual framework and literature review, Business History, 61:8, 1259-1299, DOI: 10.1080/00076791.2018.1519026

14. Iskandar, A., Virma, E., & Ahmar, A. S. (2019). Implementing DMZ in improving network security of web testing in STMIK AKBA. arXiv preprint arXiv:1901. 04081.

15. What is a DMZ. https://intellipaat.com/-blog/what-is-dmz-network.