Aftab *et al.LGU (IJECI)* 2023

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 7 issue 1 Year 2023

Detection and Control over the offences of White Collar Crimes, Frauds and Hacking of information, by using effectively the relevant Software and Electronic Devices

Aftab Ahamd Malik[1], Mujtaba Asad[2] and Waqar Azeem[3]
University of Kent, England [1]
Department of Criminology and forensic Sciences, Lahore Garrison University, Lahore [1]
Shanghai Jiao Tong University, China [2]
South Eastern Regional College, Downpatrick, Ireland UK [3]
Corresponding author: dr_aftab_malik@yahoo.com
Received: November 21, 2022; **Accepted**: December 30, 2022; **Published**: March 03, 2023

Abstract

In both developed and emerging nations, fraud, white collar crime and malpractices in small and medium-sized businesses, banking, and other sectors are on the rise. The criminals are carrying out their fraud-related offence by using the most up-to-date information technology structures and similar electronic media to create unjust loss and harm in the fields of white collar crimes, banking, business, and to persons. The goal of this research paper is to make these businesses understand the need of utilizing the most up-to-date, trustworthy, and legitimate software and the necessity of making their networks more secure from external threats. The thieves are able to accomplish their goals thanks to the usage of sophisticated features for tracking and hacking private information utilizing software and information technology resources. In essence, their tactics rely on deceit and dishonesty to harm others. In essence, their methods of operation rely on deceit and dishonesty to commit the crime. Employees of the affected organisations are frequently complicit in banking and white collar scams, aiding and abetting outside criminals by transferring sensitive information. Parody, distortion, misrepresentation, twisting of the fact or truth, and concealing of actual information that is harmful to another person are all examples of fraud. The legislation's attempt to punish fraudsters seems extremely naive. There are many reasons why criminals flee, including the fact that their identities are frequently kept a secret. The criminals are able to move toward exoneration and freedom due to a lack of evidence, shoddy investigation, and naive prosecuting tactics. The fraudsters possess high quality Software Engineering Tools and Electronic Equipment to commit offences of such to harm entrepreneurs, financial organizations, commercial banks by depriving and extravtinf information and money from the concerned accounts, Technically and operationally feasible and valuable suggestions for implementation are presented in this paper to safeguard the Networks of organisations.

Keywords: Cyber Crime, Frauds, White Collar Crimes, hacking of information, Financial Crimes

1. Introduction

Mostly the malpractices occur in marketing and buying securities, hacking valuable personal information of consumers and customers and then extracting money from their bank accounts. Just only the legislation cannot help the victims. Fraudulent activity includes elements like outwardly apparent, superficial financial necessity and justification for validation and justification. Legally, the court defines fraud as a situation in which a false representation is made in order to carry out fraudulent action. Fraudulently obtaining money or "services" with the purpose to defraud is a crime. Essential components of frauds include deception, illicit gain, opportunity, purpose, and opportunity. Law enforcement organizations had not been operating at a satisfactory level. The area of frauds, particularly in accounting, society, organizations, and public, private, autonomous, and semi-autonomous bodies, has a vast amount of room for research.

Over the past eight decades, white-collar crime research has changed. The nature of “white collar crime” has also changed. Due to high-Tech and improvements are one change in the offices that has probably had an impact on white-collar crime. Particularly with the invention of the computer, both inside and outside of the office, there have been more opportunities for crime to occur. However, very few studies have looked at cybercrime from the perspective of such offences. White-Collar Crime and Cybercrime: Differences. Even if there are two distinct cancer types, this does not imply that they are the same. For instance, skin cancer and colon cancer are both types of cancers, but they have different causes, effects, and treatments.

International issues are more prevalent in cybercrime. Younger criminals are more likely to commit cybercrimes. A national threat has been created around cybersecurity. The two sorts of crime show different signs of trust. White-collar crime and cybercrime criminals' educational backgrounds might vary. It is observed that normally goals of banks similar, though they may excel more in certain specialized areas and achieve their goal and objectives. The Investment banks concentrate on attracting investors who want to invest money in the stock market and expand their financial holdings by buying and selling shares. The management of the money supply for an entire nation or set of nations is assisted by central banks. The central bank of a nation influences monetary movement, interest rates, and financial policy. Due the reputation and the measures taken by the banks, they become popular and trust worthy. In United States, the following banks are famous and considered to be safe, for their reputation:

Table 1 : Safe Banks

AgriBank	Citibank	Capital One	JPMorgan Chase
M&T Bank Corporation	PNC Bank	U.S. Bank	Wells Fargo

2. Cybercrime And White Collar Crime

According to [1] and [2[, there is difference among Cybercrime & White-Collar Crime and the papers give useful discussion on the differences also; while [3] has emphasized area of Cyber Security for Banks at great length regarding banks, industrial banks and industry itself. The paper [4] highlights very important tools used by the hackers and Fraudsters. There are indeed a dozen useful to tools used against the banks given in tables 2. Because, the gangsters are after the following information to damage the victim such as Account number, Birthdate, Location, Mother's name and other information about the account and account holder. Most of he financial crimes become easy to handle using personal confidential information. Regarding computer aided facilities available to criminal [4] presents discussion at depth and [5] speaks openly about the Cybersecurity. If difficult circumstances are encountered, the highlights have made the web a success; nevertheless, its support for modernization and free-form may be at jeopardy due to its scatter and client-controlled nature. If the lacklustre support for web features is seen as a success in and of itself, that opinion is highly subjective and influenced by the users. Even while this approach, which gives the client authority, supports the innovation paradigm, it might nevertheless pose risks to the wider public. Corruption, illegal activity, civil crime, and terrorist activity are examples of traditional ways that appear in our environment and result in bodily harm.

Information is a powerful tool. Today, government has made cyber security on top priority and a fundamental requirement. Demand for cyber security for saving foundation has significantly increased, to the point that the government has made it a priority to manage cyber risks by enhancing cyber security. Cybersecurity is essential for enhancing national security, increasing consumer confidence, and ensuring the reliability of systems that support our economy. Cybersecurity accomplishments must be carefully adjusted in order to protect privacy, freedom, alteration, and the motivating nature of the Internet. To create an effective and equitable cyber security plan, each component of the nation's essential framework must be taken into account separately.

Table 2: Toolkits of gangsters and fraudster Ref: [8]

Computer pop-ups	Fake claims	Fake entities	Fake names, credentials, numbers
Fake photos	Fake profiles	Lead lists	Persuasion
Robocalls	Phishing	Secrecy	Spoofing

3. Banking Software

Banks are confronting with different applications in their normal routine work and hence require differe nt types of software, especially related to online running the system. Today, the mainstream of people and organizations have some kind of financial account in banks. The

banking system software is indeed very complicated and sometimes is naïve and needs updated versions. The formal utilities, debugging software and usual operating systems require repairing and revamping in order to standardize the functionality and its ability cope up with new requirements. On the other hand, the banks and customer's company, both use Computerized Management Control and Information Systems which requires compatible software for storage, processing and retrieval purposes.

The famous firms, who develop sophisticated banking encryption software are given in Table 3 and Table 4 provides a few best banking software. In Table 5. we list some important Encryption Algorithms, where, AES is "Advanced Encryption Standard", also considered to be the best for US-banking and other entrepreneurs. There are several best banking software available in market for various applications for Computer Systems, Management, Corporate Banking, handling Bank Administration, and daily banking application systems. JIRA is one of the best Banking Software System to perform various important banking tasks such as Project Management, works as a tool for management, portfolio, product-management, for local configuration systems ,Portfolio and asset-management tool and also as testing-tool. Originally, it was developed by an Australian famous company. Table 6 provides the best "Software names" for online and other Banking applications.

3.1. Online Banking Software

The users may be benefited by several reliable software in the area of on-line banking. One of the trusted software, which is cloud based, can be used for "accounting Management"; it is helpful to program and automate the payable processes. Tipalti is one of the cloud based software. Some other effective and useful software are given in Tables 8. There is another cloud based software known as Fraud.net; which is used for risk management platform. It provides tools for fraud prevention.

Table 3 Encryption software developing companies for banks

IBM Corporation	Avaloq	Trend Micro Sophos	Thales Group

Table 4 Best Software for banking applications

Avaloq banking suite	CGI open finance	Core banking	Flexcube
Oracle	SAP for banking	Symphony™	TCS bancs
Temenos transact	TurnKey Lender	Validis	Mambu

Table 5: Best Banking Encryption Algorithms

AES	Blowfish	Tripple DES	Twofish	Rivest-Shamir Adleman (RSA)

Table 6: Best Software names for online and other Banking applications

Bank Account opening	Bank Account Tracking	Bank Account Management	Bank Budgeting
Bank Compliance	Banking Contract Management	Cash Management for Banks	Electronic Banking
Gnucash Online Banking	Home Banking	Kmymoney Online	Mobile Banking
Online Account Opening	Quickbooks Online Banking	Quicken Banking	Quicken Online Banking

Table 7: Suitable Software for Core Banking System

CBC Core Banking System	Cloud based core	Equation core	Finacle	Flexcube	HSBC

Table 8: Software for Online Banking

Centrex	Cyberbank	FinCell	Fraud.net
Origins	Plaid	The Nortridge Loan System	Tipalti

4. Protective Measures To Safeguard Banking Information From Fraudsters

With fast developments in Information Technology and recent research in Software Engineering, the entrepreneurs and financial organizations may choose a most suitable and feasible solution to safeguard their precious data and applications as well as the "System Software" from outside attacks. It is important to adopt preventive security measures before the damage occurs. Most obvious source of problems and criminal activities is the "Internet". Now most of the companies have their own dedicated intranets and extranets. By an intranet, the outsider is allowed to moderately access the company's network in secured manner. Mainly the intranets are used by the employees of the organization; whereas the extranets allow the outside business associates or customers having stakes in the organization. According to [5], there several protective measures to protect the banks from hackers and criminal gangsters. The Cybercrime are committed online by breaching the personal information of customers, what is termed as "Identity Theft'. It is well known that the terrorists are frequent user of internet; particularly the "mobile-terrorists". The terrorist's feat and take advantage of the weaknesses and bugs in the software. The use of digital devices by criminals have been described at length in [6]. The authors of [6] recommend for the implementation of stronger electronic devices to combat with Cybercrimes and white Collar Crimes. The paper [7] strongly recommends the use of a "Demilitarized Zone" in Network

to provides a protective measure to the network by using a "hardware fire wall", a "software firewall" with routers so that the signals from outside hackers are identified and killed on the spot. In Table 9, there is a list of a few Internet Security Software, which have been found useful:

Table 9: Internet Security Software

Avast Premium Security 2020
Kaspersky Total Security 2020
McAfee Total Protection
Symantec Norton Security Deluxe
Webroot Internet Security Complete with Antivirus Protection
Webroot Internet Security Plus with Antivirus Protection

5. Recommendations

Banks now confront new security issues as a result of the rapid expansion of their attack surfaces due to digital transformation. The average rate of attack on banking is increasing day by day. The financial companies and the banks are attacked about a thousand times fortnightly. Therefore, strict measures according to the recommendation of [6] and [7] must essentially be adopted. More recommendations are put forward below.

i. Installation of a "Demilitarized Zone" in Network provides effective security.

ii. The users must seek help from academia and software industry to get resolved their problems.

iii. Installation of a "virtual private network VPN" has been found useful to guard and provide a shield to the online "sending" and "receiving" the Data during the usage of "public Wi-Fi". The SD WAN is very useful for banks connected with their braches. It is software which protects and secures the work of the branches connection with internet and clouds.

iv. The use of Cloud Guard provides full, wide-ranging and comprehensive security to the users of e-banking.

v. Enhance the internet security measures for your installation.

vi. If the attack has occurred, soon after without wasting time, inform to your bank or organization. Let them know the details about the fraud and your "identity-theft".

vii. A complicated pass-word must be used consisting of alpha-characters, numerics and special characters. Its length must be 10 characters.

viii. Continue to change your password over time

ix. Never conduct online banking on a public computer

x. When conducting online banking, only use trusted apps or websites

xi. Ensure that you only use safe internet connections

xii. Avoid being a victim of phishing

xiii. Protect your PC.

xiv. The settings of social media must be kept updated to avoid any harm.

xv. The updated versions of application software, operating systems and Security software must always be used.

xvi. All the identity information must be kept under lock. Protect yourself.

xvii. It is advised by FBI, that people must not use fake and false banking apps, which are prepared to harm the users while the trackers commit cybercrimes

6. Acknowledgements

The authors are grateful to Mr Kaukab Jamal Zuberi, Head of Department of Criminology and Forensic Sciences for his guidance and useful discussion; also to the Chief Editor for encouragements.

7. References

[1]. R. Eric and R. Thompson, "Computer Facilitated White-Collar Crime : Computers & Criminal Justice". https://cod.pressbooks.pub/crimj1165/chapter/-module-7-computer-facilitated-white-collar-crime/

[2]. Cyber Security for Banks, https://www.checkpoint.com/industry/banks/

[3]. L. Vitalise, "Top 10 Best Internet Security Software", https://www.consumersearch.com/technology

[4]. K. Brian and Payne, "White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both? " ., vol. 19, no. 3, pp. 16–32. Criminology, Criminal Justice, Law & Society E-ISSN 2332-886X https://scholasticahq.com/criminology-criminal-justice-law-society

[5]. A. G. Johansen, "11 ways to help protect yourself against cybercrime", NortonLifeLock. 2020.

[6]. A. A. Malik, "Bank Frauds Using Digital Devices and the Role of Business Ethics", IJECI., vol. 2, no. 4, pp. 21-32. 2018.

[7]. A. A. Malik, M. Asad and W. Azeem,"-Frauds In Banking and Entrepreneurs by Electronic Devices and Combating using Software and Employment of

Demilitarized Zone in the Networks", IJECI. vol. 1, no. 1. 2023.

[8]. Katherine Skiba(2022), " 12 Tools in a Fraudster's Toolbox", EN ESPANOL