

Think India Journal

ISSN: 0971-1260 Vol-22, Special Issue-21

National Conference on

Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by

Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62

Held on 4th January 2020



Cyber Crime in Banks

R.D.KARTHICK,

Assistant Professor, Vel Tech RangaSanku Arts College, Avadi.

ABSTRACT

In 1990's People can easily identified the crimes due to physical presence but after the boom of internet even police can suffered a lot to find the victims. Basically the crimes are done by ethical hackers who are highly knowledgeable in computer and know the dark side of it. Here the article gives an attempt to study the various crimes which are all in banking sector especially cyber-attacks and the interesting part is till now there will be no hackers can officially caught by the departments in our country.

INTRODUCTION

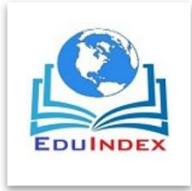
Internet now a days pupil will be without food and water but they can't imagine without internet because it the place where we get complete communication and access information of gaming, online shopping, studying, social networking, online jobs, etc. pupil also same the soft copier of their identity documents like PAN, Aadhar, Driving License even education certificates in Google drive by scanning. Which gives complete and safe access from anywhere at any time. Here comes the real fact, what happens if the mail id and password missed or forgot or known by some other persons?

Mail id and password known by stranger, who as a hacker is the biggest and updated problems in India. Criminals are mostly exploiting the speed, convenience of the internet frauds due to credit and debit cards, illegal downloading, child pornography, distribution of virus, etc.

CYBER LAW IN INDIA

- IT Act (Information technology Act)
- IPC (Indian Penal Code)
- State level Legislation Act

By these 3 cyber law fraudulent may be caught and punished. Online frauds activities are difficult to find out. Even though the victims got arrested the fund lost is lost. The ministry of



Think India Journal

ISSN: 0971-1260 Vol-22, Special Issue-21

National Conference on

Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by

Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62

Held on 4th January 2020



Home affairs to the State government has cyber police station, trained man power with terminal infrastructure for detection, investigation, prosecution of cybercrime.

TYPES

Two types of cyber crime

- Spoiling the computer network by loading, virus transferring, etc.
- With the computer is used as weapon like cyber terrorism, money laundering, fraud of credit card, IPR, etc.

Salami attacks are done for financial crimes like if employee of bank inserts a program to deduct Rs.4.00/- from each account an every month but the account holder monthly not notices it and the employee makes sizable amount every month.

Online gaming is used for **Hawala transactions**, money laundering, etc.

E-COMMERCE ON INTERNET FRAUDS

It is an offer that was false claims to solicit loan or investment that provides or counterfeit securities, etc.

CYBER CRIME IN BANKING SECTOR

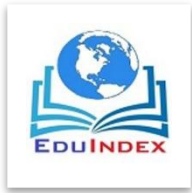
Out of top 10 countries India ranked 4th by cyber attackers. Cyber-attacks are an illegal activity and are continuously increase in India for financial loss. It is an attempt to destroy computer network to extort money and necessary information.

MAJOR CYBER ATTACKS IN INDIA IN 2018

SIM SWAP FRAUD in Aug 2018 two from Navi Mumbai arrested – Carrying out transactions through online banking they hacked nearly 4 cores rupees from various accounts.

CYBER ATTACK ON BANK in Aug 2018 Pune branch, nearly 94 cores rupees being siphoned off they hack the main server of bank and also ATM Servers.

CANARA BANK ATM HACKED in Kolkata in July 2018. Hackers used skimming device on ATM card holders, they wiped off almost 20 lakhs rupees from various bank accounts.



Think India Journal

ISSN: 0971-1260 Vol-22, Special Issue-21

National Conference on

Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by

Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62

Held on 4th January 2020



WEBSITE HACKED over 22000 websites were hacked between the months of April 2018. As per the information given by Indian Computer emergency Response Team (CERT-IN) over 49 websites were affected by malware including 114 websites run by government. These attacks done with the help of gathered information and the details of the users of bank accounts through the Aadhar Number.

REASONS FOR CYBER CRIME IN BANKING SECTOR

At least one cybercrime was reported every 10 minutes in India in 2018. It was increased in 2017, reporting time will be 12AM in India has seen a total of 1.7 lakhs cybercrime in part 3 – 4 years.

The real Tragedy is police not lodging the FIR for First 3 months. To disgusting that a common man who losses his money without his knowledge now can't even file an FIR when a crime is committed against him.

The main reason for India as the cybercrime in banking sector has it has rapid population growth and number of internet users increase years wise, nearly 20 corers population using social media very actively in a day in India.

- Lack of awareness and easy access using auto saved passwords in system or mobile phones using Google accounts.
- Bank accounts linked with UADAI and PAN numbers, so that data can be transferred very quickly related to finance.
- People do not know what is hacking and how are can took the money with using Technology. No education can teach this or how to prevent from this kind of problems.
- People shared their details like Date of Birth, Home Address, Credit card information, EMI amount, Account Number, signature, Passwords in mobile contacts. So those, hackers can easily get through one call and one number.

HOW TO SECURE FROM THESE CYBER CRIMES

LPA

Least Privileged Accounts exclusively use LPA on Computer. Theses profiles do not need administration access, nearly 2/3 of vulnerabilities could be prevented by the use of an LPA.



Think India Journal

ISSN: 0971-1260 Vol-22, Special Issue-21

National Conference on

Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by

Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62

Held on 4th January 2020



PASSWORDS

The most common password used in India in “1234” a report says by IOB in 2017. Some pupil kept their birth year as passwords or their child name as a password which is easily for hacker to find and loot the money.

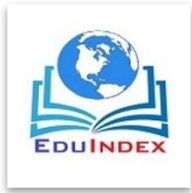
VPN

Virtual Private Network use VPN in all public networks free Wi-Fi will get from railtel, hotels, etc. but using free Wi-Fi our data becomes extremely vulnerable.

AN UNETHICAL CYBER CRIME STORY

Mr.A, has a habit of read Newspaper, fortunately he saw one Advertisement, related to Subscription of newspaper for 1 year at Rs.100/-. So he contacts the number which is mention in the advertisement and makes an appointment at next day. Sales person reaches the Mr.A home and explain about the details and ask for to pay Rs.100/- only in bank cheque not in cash. So Mr. A gives Rs.100/- cheque to sales person, after 3 days Mr. A got SMS that his account was debited Rs.7 lakhs. After getting SMS from bank Mr. A approach the banker and they confirmed that, there was a debit of Rs. 7,00,000/- through the Cheque which was given by Mr. A to salesperson.

After that Mr. A contact the newspaper company about the advertisement. The editor confirmed there is no such kind of subscription right now. So Mr. A file a complaint in police station, the police team reaches the bank to check the CCTV camera for who deposited the cheque. One 12 years small boy deposit the cheque at that time, that boy is working in local tea shop which police enquired the 12 years boy and the answer is very depressed by them. The boy said, one uncle shows teddy bear doll and if I deposit the cheque to this bank he will give that Teddy bear doll to me. So I did and the uncle face is covered by “Narendra Modi ji Image”. At the end of the investigation cybercrime team confirmed that, there is a erasable pen was used in the cheque at the time of Mr.A filled the cheque leaf. So, even such a small thing can make the people financial loss. Be Aware.



Think India Journal

ISSN: 0971-1260 Vol-22, Special Issue-21

National Conference on

Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by

Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62

Held on 4th January 2020



RECOMMEDATION TO PREVENT CYBERCRIME

- Cyber fraud council in banks
- Customer education
- Strong encryption and Decryption Methods

Cyber fraud council in banks

Whenever cybercrime happen, the victim should report to the cyber fraud council that must be setup in each and every branch of banks. This is mainly due to fact that there is a cross over between national criminal groups on their behalf with the same people working in cybercrime activities. Be reigniting the crime by the customer. The police can easily identify the criminals in minimum time.

CUSTOMER EDUCATION

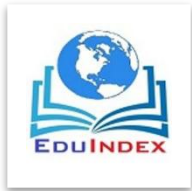
Educate the bank customers at least once in a month and keep the KYC information very safe and advice the customers never give away to someone of Sim cards, Passwords, Pin Number, Signature, Cheque leaf details, etc. because the cyber criminals can use their information to find the transaction details and they easily transfer the fund from one account to another account. If the customer need help related to cyber world, they can contact **toll free number which is 9968600000** for more clarification.

STRONG ENCRYPTION AND DECRYPTION METHODS

Strong encryption method shows like the data most encrypt using the strong random key using the CBS Technology. This technology generate the random key to use as a password to open or view the data of the customers without the random key even the account holder its of can't open or view the account data and also every time the codes must be ask to reset again to login for not time. So that are cannot easily crack the account details. It will be easy for customers view but it is an extra work for bank personnel.

CONCLUSION

Day by day technology has been developing so, criminals did not want to rob the bank nor do they have one laptop with internet connection with criminal computer knowledge. Even cyber law is not so strong in our county and fearful judgment was also not so often happened. Internet also presents national security concerns since internet serves the important and emerging



Think India Journal

ISSN: 0971-1260 Vol-22, Special Issue-21

National Conference on

Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by

Department of Commerce, VEL TECH RangaSanku Arts College,
Avadi, Chennai-62

Held on 4th January 2020



roles in banking, energy, telecommunication, petroleum, etc. As technology develops, the law needs to respond to the new development to data those who would able use and misuse the new technology.

BIBLIOGRAPHY

- www.testbytes.net
- <https://law.jrank.org>pages>computercrime>
- <https://www.unudc.org>cybercrime>
- <https://www.sciencedirect.com>topics>
- <https://itstillworks.om>examples-cybercrime>