*Published by SR Yettish*

***We try to produce the most beautiful books possible, and we are extremely concerned about the impact of our manufacturing process on the forces of the world and the environment as a whole. Accordingly we made sure that the paper we used contains 30% post-consumer and recycled fibre and 65% has been certified as coming from forests that are managed to ensure the protection and wildlife depend on them.***

***ISBN ; 9798508405243***

Don’t take rest after your first victory because if you fail in second, more lips are waiting to stay that your first victory just was luck

- ABDUL KALAM

Yesterday is history,
Tomorrow is mystery,
Today is gift,
Then what is present.

- JOKER

Don’t wait for tomorrow because it’s going to fool you, make your yesterday dreams to come true. Work for that, you will approach it.

- YETTISH SR

***This story does not interpit or hurt anyone’s opinion or any individual person.***
***Sorry if anyone gets hurt in this story***

***Thanks to all supporters who helped me in hard times.***

***Notice: The characters and events in this book are fictional and created out of imagination of the author. Certain real locations and institutions might be mentioned, but the characters and events depicted are entirely fictional.***

***Disclaimer: The publisher and author cannot be held responsible for injury, mishap or damages incurred during the use of or because of the information or words in this book.***

# *ALSO BY YETTISH SR*

***Strengthen Squad***
***Chapter  – 1, 2.***

***What's going to be next***
***Chapter  – 1, 2.***

***The real life story of great living legend Virat Kohli.***

We have seen in many movies and also read many stories about technology hacking. Is it easy to hack a bank?

Most of your answers would be definitely no. But here it happened. Actually in most of the movies and stories, the hacker will hack money from some bank accounts for every hour. But here it's somewhat different.

In this story, hackers are not going to hack an account instead of it they are going to hack the bank.

In this bank they are not going to hack $5000 or $10000 instead of it they are going to hack $351 million.

They cleaned all the money in bank. Just say me the truth how many of you guys have minimum $50,000 in your bank as saving. For example if a person has $100,000 in his bank as saving. Hacker is going to hack 700,000 people’s money to reach his destiny.

So, in which country would the hackers hack the bank? Your answer would be America, Australia or country’s which is developed well.

No, your answers are wrong. They hacked in Bangladesh a developing nation which shares its borders with India. You can also ask that hacking a bank is not simple.

Yes hacking a bank is not possible. So, he has to do international transaction. Doing an international transaction is not simple as possible.

If a bank does an international transaction it should do only by the process of SWIFT (Society for Worldwide Interbank Financial Telecommunications).

Also SWIFT won't transfer moneys, it only transfers payment order's that is only messages. The receiving bank will processes payment requests.

You do have a doubt that how this makes a hack, also do they hack both the banks. So, what's going to be next?

Bangladesh is a place where Muslims live as majority. So, Bangladesh had their government holidays or weekends on Friday and Saturday, which means Thursday was their last working day.

***Let's go deep***
February 7,
It's time for hackers.

On Thursday night hackers entering Bangladesh's banking system and initiating their transaction through Swift. This money was transferring to America's Federal Reserve Bank.

So, the next is Friday. America's Federal Reserve Bank processed requesting transaction according to their SWIFT method.

They started to send the moneys to different places in the world. Bangladesh was not cautious about this because it was their official holiday for all the employees.

So, the next day Saturday both Bangladesh and America had their official holiday. So, the next day it’s Sunday official working day for Bangladesh’s employees. On that day they came to know about this transaction.

Almost $951 Million has transferred from their bank. Immediately Bangladesh planned to send a message to stop the payment orders to America Federal Reserve Bank through SWIFT.

America Federal Reserve Bank can’t do anything because it was official holiday for them.

So, the next day Monday both the countries had their official working day. After seeing the stop payment request from Bangladesh, America Federal Reserve Bank was trying to send a message to Philippine National Bank.

Philippine National Bank was the most important bank because more money was sent to that bank. But unfortunately it was china’s New Year, Philippine National Bank won’t work.

***Which means no one can stop the payment.***

This bank was also the official bank for Bangladesh which means government runs this bank. The main branch was situated in Dacca, Bangladesh Capital.

So, to go in deep what happened there? How did the hacker hacked the banking system and SWIFT password and accounts? We all get answer here.

On February 7, Director of central bank came to the office backside (the most secure place). Account holders can’t go there. Why the Director of central bank should go there?

Director of central bank came there because the printer was not working.

You can ask that if a printer is not working means should a Director come? It's not just a printer. This printer was automated printer connected to SWIFT network.

This printer prints the live transaction for 24/7. From the morning transaction is going on but the printer did not printed transactions.

So, the printer had some glitches. Immediately, employees called the technicians. Almost the quarter day ended with this problem.

So, printer gets ready and printed all the transaction. After seeing the transaction "boom boom boom" it was like that to all the bank employees.

Totally 35 transaction has happened on Thursday night. Each transaction had big amounts such as $30-$20 million. All the transactions took place through the SWIFT network.

Many banks, institutional, etc. are sending their money through SWIFT as their official mode to transfer moneys.

Bangladesh bank employees still don’t know how the hackers did this, because SWIFT has more power privacy.

I don’t know how many of you know this, when a bank sends an international transaction it is checked by a country as a routing bank.

Bangladesh bank workers sent a request through SWIFT to America Federal Reserve Bank in New York.

Like many other national banks, Bangladesh Bank, the central bank of Bangladesh, maintains an account with the Federal Reserve Bank of New York to deposit maintain, and transfer foreign currency reserve of Bangladesh.

The foreign currency reserve of Bangladesh, a growing economy, often reaches multiple billions of US dollars.

As of September 2020, Bangladesh has a foreign currency reserve of US$39 billion.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) network is used to communicate with the bank holding the foreign exchange account in order to withdraw, transfer, or deposit the currency.

Hackers hacked the foreign currencies in Bangladesh. May be it is foreign currencies but its people’s money. All the pressure will hang on Bangladesh’s Bank.

America Federal Reserve Bank got a request from Bangladesh bank to transfer the 35 transaction to different places of the World.

There were two different problems here:

1. This request came at Thursday’s night, the next working day Friday. America has reviewed all the requests, which means they have transferred all the moneys.

2. The stop payment request was sent on Sunday, America’s official holiday. So America got this news on Monday.

Before going to climax, we all need to know how the hacker hacked SWIFT network. Also I want to ask you guys how much you read well?

Recalling is very important for my books, because it’s a crime novel that’s why. If you know all the incidents, it’s well and good if not go back and read it well.

## *Hacker's idea*

On January that is February the incident happened, 15-20 days before. Bangladesh central bank workers received an email, sent by hackers. Without knowing it workers clicked it and malwares started to download.

The malware was noticing all the privacy of Bank including SWIFT credentials. The malware job was to record and send to the Hacker.

So, now the hacker knows the password and log in details of SWIFT. Now it's easy for the hackers to take money.

As already said on February 4 Thursday night they are logging into SWIFT credentials and initiating the transactions and also hacking the Printer.

Luckily 30 transactions flagged because it had some spell errors and also those transaction was kept on hold that is keeping it in manual review.

So, 30 Transaction has been flagged so remaining 5 has been proceeded by America Federal Reserve Bank.

The 5 transaction had $101 million, 1st transaction had in Pan Asia Bank in Sri Lanka. The user was Shalika Fundation.

Don't say you made a spell error, it's a spell error made by the hackers. It was registered as non-profit account and also registered as NGO (Non-Governmental Organization).

As I said international transaction don't goes directly to a person's account.

In fact, there is a routing bank between them. Sri Lanka had a routing bank called as Deutsche bank in Germany. They stopped the transaction because of the spell error 'fundation', also NGO can't get $20 million easily.

So, Routing bank also getting confirm from America Federal Reserve Bank on Monday. The America Federal Reserve Bank also said to stop the transaction. So, the remaining four Transaction $81 million have sent to RCBC bank in Philippines.

As I said before itself Monday was China’s New Year. Hackers withdrawn $58.15 million, and they were to be put into Casino’s money Laundry.

Still no one knows who was that, also I researched about account in deep. The four accounts was also a fraudulent ID’s.

To know in detail these are the investigation.

***Bangladesh,***

Initially, Bangladesh Bank was uncertain if its system had been compromised. The governor of the central bank engaged World Informatix Cyber Security, a USbased firm, to lead the security incident response, vulnerability assessment and remediation. World Informatix Cyber Security brought in the forensic investigation company Mandiant, for the investigation. These investigators found "footprints" and malware of hackers, which suggested that the system had been breached.

The investigators also said that the hackers were based outside Bangladesh. An internal investigation has been launched by Bangladesh Bank regarding the case.

The Bangladesh Bank's forensic investigation found out that malware was installed within the bank's system sometime in January 2016, and gathered information on the bank's operational procedures for international payments and fund transfers. The investigation also looked into an unsolved 2013 hacking incident at the Sonali Bank, wherein US$250,000 was stolen by still unidentified hackers.

According to reports, just as in the 2016 central bank hack, the theft also used fraudulent fund transfers using the SWIFT global payment network. The incident was treated by Bangladeshi police authorities as a cold-case until the suspiciously similar 2016 Bangladesh central bank robbery.

## *Philippines*

The Philippines' National Bureau of Investigation (NBI) launched a probe and looked into a Chinese-Filipino who allegedly played a key role in the money laundering of the illicit funds. The NBI is coordinating with relevant government agencies including the country's Anti-Money Laundering Council (AMLC).

The AMLC started its investigation on February 19, 2016 of bank accounts linked to a junket operator. AMLC has filed a money laundering complaint before the Department of Justice against a RCBC branch manager and five unknown persons with fictitious names in connection with the case.

A Philippine Senate hearing was held on March 15, 2016, led by Senator Teofisto Guingona III, head of the Blue Ribbon Committee and Congressional Oversight Committee on the Anti-Money Laundering Act. A closed-door hearing was later held on March 17. Philippine Amusement and Gaming Corporation (PAGCOR) has also launched its own investigation. On August 12, 2016, RCBC was reported to have paid half of the Ph₱ 1 billion penalty imposed by the Central Bank of the Philippines. Prior to that, the bank reorganized its board of directors by increasing the number of independent directors to 7 from the previous 4. On 10 January 2019, Maia Santos Deguito, a former manager at RCBC was convicted and sentenced to 4 to 7 years imprisonment at a Philippine court for money laundering.

On 12 March 2019, RCBC sued Bangladesh Bank for embarking ”on a massive ploy and scheme to extort money from plaintiff RCBC by resorting to public defamation, harassment and threats geared towards destroying RCBC's good name, reputation, and image.”

***New York***

FireEye's Mandiant forensics division and World Informatix Cyber Security, both US-based companies, investigated the hacking case.

According to investigators, the perpetrators' familiarity with the internal procedures of Bangladesh Bank was probably gained by spying on its workers. The US Federal Bureau of Investigation (FBI) reported that agents have found evidence pointing to at least one bank employee acting as an accomplice.

The FBI also alleged that there is evidence that points to several more people as possibly assisting hackers in navigating the Bangladesh Bank's computer system.

The government of Bangladesh has considered suing the Federal Reserve Bank of New York in order to recover the stolen funds.

WRITTEN BY

Yettish SR

A Legends Production