Ecommerce Security: Familiarization: Online Banking Security, Mobile Banking Security, Security of Debit and Credit Card, UPI Security.

COUNTER CYBER SECURITY INITIATIVES IN INDIA

To counter cyber security attacks, Government of India have taken some initiatives which are listed below:

1. **National Counter Terrorism Center(NCTC):** After 26/11 attack in 2008, suddenly the Indian government realized the importance of Counter terrorism initiatives and proposed National Counter Terrorism Center(NCTC) to provide intelligence inputs to the decision makers to plan for counter terrorist activities. The NCTC is supposed to coordinate between various State and Central govt. agencies and serve as a single and effective point of control and coordination of all counter terrorism measures. It is modeled on the American NCTC and Britain's Joint Terrorism Analysis Centre and will derive its powers from the Unlawful Activities Prevention Act, 1967 (Mrunal, 2012).
2. **National Information Security Assurance Programme (NISAP):** To create the awareness among the people in the government and critical sector organization, CERT-In has taken an initiative called National Information Security Assurance Programme (NISAP), to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. CERT-in has established the facility for Computer Forensics for investigation of cyber crimes and to provide hands on training to the law enforcement agencies and judiciary. This infrastructure is being augmented to include network forensics and mobile forensics investigation facility. CERT-In is cooperating with defence, banks, judiciary and law enforcement agencies in training their officials as well as extending the support in investigation of cyber crimes (Srinath, 2006).
3. **Computer Emergency Response Team-India(CERT-In):** The Indian Computer Emergency Response Team was created in 2004 by Department of Information Technology. The purpose of creating CERT-In was to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country and is also responsible for overseeing administration of the IT act (CERT-In, 2014).
4. **Indo US Cyber Security Forum (IUSCSF):** The India-US Cyber Security Forum was established in 2001 and is dedicated to protecting the critical infrastructure of the knowledge-based economy. The members of the forum are various government and private sector organizations, both from India and the United States, working under the Forum's auspices, have identified risks and common concerns in cyber security and crafted an action-oriented work plan on securing networked information systems. The Forum focuses on cyber-security, cyber-forensics and related research and works towards enhancing co-operation among law enforcement agencies on both sides in dealing with

cyber crime. Defence services of both the countries will enhance their interaction through exchange of experience in organizational, technological, and procedural aspects. Ongoing co-operation between India's STQC and the US National Institute of Standards and Technology (NIST) will expand to new areas including harmonization of standards. CII and their US counterpart have decided to set up an India Information Sharing and Analysis Centre (ISAC) and India Anti-Bot Alliance ('bot' refers to software that can be tasked to invade computers and undertake malicious activities remotely on behalf of hackers) (Press Information Bureau, 2006).

5. **National Critical Information Infrastructure Protection Centre (NCIPC) of India:** It is declared as a nodal agency for the protection of critical information infrastructure of India and is responsible for all measures including R&D for protection of critical information infrastructure. Some of the activities that NCIIPC performs are (Chander, 2013):
    1. Identification of Critical Sub-sectors
    2. Study of Information Infrastructure of identified critical sub-sectors
    3. Issue of Daily / Monthly cyber alerts / advisories
    4. Malware Analysis
    5. Tracking zombies and Malware spreading IPs
    6. Cyber Forensics activities
    7. Research and Development for Smart and Secure Environment.
    8. Facilitate CII owners in adoption of appropriate policies, standards, best practices for protection of CII.
    9. Annual CISO Conference for Critical Sectors.
    10. Awareness and training
    11. 24X7 operation and help-desk
6. **National Intelligence Grid (Natgrid) project of India:** It is the integrated intelligence grid developed by C-DAC-Pune connecting databases of core security agencies of the Government of India (C-DAC, 2014). It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel (Yasmeen, 2013). This combined data will be made available to 11 central agencies, which are: Research and Analysis Wing, the Intelligence Bureau, Central Bureau of Investigation, Financial intelligence unit, Central Board of Direct Taxes, Directorate of Revenue Intelligence,Enforcement Directorate, Narcotics Control Bureau, Central Board of Excise and Customs and the Directorate General of Central Excise Intelligence.
7. **Crime and Criminal Tracking Networks and Systems (CCTNS) project of India:** It is a project under National e-Governance Plan(NeGP) covering all 28 States and 7 UTs which aims at creation of a nation-wide networking infrastructure for evolution of IT-enabled sophisticated tracking system around 'investigation of crime and detection of criminals (PTI, 2013). The goals of the CCTNS are to facilitate collection, storage, retrieval, analysis, transfer and sharing of data and information at the police station and between the police station and the State Headquarters and the Central Police Organizations. CCTNS would provide a comprehensive database for crimes and criminals, and it would be easier for the law enforcement agencies to track down a criminal moving from one place to another.

8. **National Cyber Coordination Centre (NCCC):** National Cyber Coordination Centre is a proposed cyber security and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Some of the components of NCCC include a cyber attack prevention strategy, cyber attack investigations and training, etc.
9. **Botnet Cleaning Center:** As a part of the Digital India programme, the Government is setting up a centre that will detect malicious programmes like 'botnets' and help people remove such harmful softwares from their devices. " The Government is setting up 'botnet' cleaning and malware analysis centre" according to media reports. Botnet is a network of malicious software. It can steal information, take control of device function and carry out cyber attacks like Distributed Denial-of-Service (DdoS).
10. **E-mail policy of Government of India:** In present date Email is considered to be as the major source of communication between individuals and organization as well. The same applies to Govt. of India (GOI) as well. E-mail has become major mode of communications for the entire government. With the increasing use of Emails to communicate among different Govt. Agencies, the Email Policy was laid down by Government of India (GOI) in October 2013. Here we will cover some of the important clause of policy, readers are advised to download policy from Department of Electronics and IT website.
11. **Ministry of Home Affairs (MHA):** The Ministry of Home Affairs (MHA) is a ministry of the Government of India. An interior ministry, it is mainly responsible for the maintenance of internal security and domestic policy. Readers are advised to read annual report of the Ministry of Home Affairs. The Ministry of Home Affairs (MHA) has multifarious responsibilities, the important among them being-internal security, border management, Center-State relations, administration of Union Territories, management of Central Armed Police Forces, disaster management, etc.
12. **National Crime Records Bureau (NCRB):** NCRB shall endeavour to empower Indian Police with Information Technology and Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery. This shall be achieved through coordination with police forces at National & International level, upgradation of crime analysis technology, developing IT capability & IT enabled solutions.
13. **Data Security Council of India (DSCI):** Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. To further its objectives, DSCI engages with governments, regulators, industry associations and think tanks on policy matters. To strengthen thought leadership in cyber security and privacy, DSCI develops best practices and frameworks, publishes studies, surveys and papers. It builds capacity in security, privacy and cyber forensics through training and certification program for professionals and law enforcement agencies and engages stakeholders through various outreach initiatives including events, awards, chapters, consultations and membership programs. DSCI also endeavours to increase India's share in the global security product

and services market through global trade development initiatives. These aim to strengthen the security and privacy culture in the India.

Securing Online Banking

Most industries have deployed internet technologies as an essential part of their business operations. The banking industry is one of the industries that has adopted internet technologies for their business operations and in their plans, policies and strategies to be more accessible, convenient, competitive and economical as an industry. The aim of these strategies was to provide online banking customers the facilities to access and manage their bank accounts easily and globally.

Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

Online banking has been deployed more frequently over the past few decades to support and improve the operational and managerial performance within the banking industry.

Threats to Online Banking

There are some information security threats and risks associated with the use of online banking systems. The confidentiality, privacy and security of internet banking transactions and personal information are the major concerns for both the banking industry and internet banking. Attacks on online banking today are based on deceiving the user to steal login data. Phishing, pharming, Cross-site scripting, adware, key loggers, malware, spyware, Trojans and viruses are currently the most common online banking security threats and risks.

The following are the major attack scenarios:

- A credential stealing attack (CSA), is where fraudsters try to gather user's credentials, either with the use of a malicious software or through phishing.
- A channel breaking attack (CBA), involves intercepting the communication between the client side and the banking server, by masquerading as the server to the client and vice versa.

- A content manipulation also called man-in-the browser (MiTB) attack, it takes place in the application layer between the user and the browser. The adversary is granted with privileges to read, write, change and delete browser's data whilst the user is unaware about it.

Best practices for online Banking Users

For Users

Protect your PC:

- Install anti-virus software and keep it updated on a regular basis to guard against new viruses
- Install anti-spyware security software against those programs that monitor, record and extract the personal information you type in your PC (passwords, card numbers, ID numbers, etc.)
- Install personal firewalls to protect your PC against unauthorized access by hackers
- Keep your operating system and internet browser up to date, checking for and downloading new versions/security enhancements from the vendor's web site

Protect your personal information:

- Create hard-to-guess security access codes (User ID & password) for Online Banking and make them unique (e.g. they should not be the same as those you use to access your e-mail account)
- Change your security access codes periodically
- Memorize your security access codes, avoid writing them down and keep them strictly personal and confidential
- Do not disclose to ANYONE your security access codes: Bank will never initiate or contact you for your e-banking or ATM PINs, card or account numbers, personal identification information, neither over the phone nor in any electronic or written message. Also refrain from providing ATM pin for ecommerce transactions.
- Never leave your PC unattended when logged into Online Banking
- Always remember to log off from your online session using the "Log-off" button when finished using the e-banking services

Use the Internet cautiously:

- Always access Online Banking internet only by typing the URL in the address bar of your browser.
- Never attempt to access Online Banking internet through an external link of unknown or suspicious origin appearing on other websites, search engines or e-mails
- Before logging in, check for the Bank's Security Certificate details and the various signs (e.g. green address line and Lock, HTTPs) that confirm you are visiting the secure pages of Bank.
- Ignore and delete immediately suspicious fraudulent (phishing, spoof, hoax) e-mails that appear to be from Bank, asking you to urgently click a link to a fraudulent (spoof) website that tries to mimic the Bank's site and to lure you into giving out your sensitive personal information (PIN, account or card numbers, personal identification information et al.)
- Never click on a link contained in suspicious e-mails
- Avoid using Online Banking from public shared PCs (as in internet cafes, libraries, etc.) to avoid the risk of having your sensitive private information copied and abused

Stay alert:

- Sign-on to Online Banking regularly and review your account transactions, checking for any fraudulent activity on your account (e.g. transactions you do not recognize)
- Keep track of your last log-on date and time, displayed at the top left side of the Online Banking Home page
- Once logged into Online Banking, you can also monitor the actions performed online

Prompt reporting of suspicious activity:

- Contact your bank immediately, if you think someone knows your security access code or in case of theft of your code/ money or in case you have forgotten your credentials.
- Forward any suspicious e-mails to the bank on their phishing reporting email as well as on CERT-In email incident@cert-in.org.in
- Your prompt action is crucial to prevent any (further) damage

Reference:

http://www.cert-in.org.in/

Securing Mobile Banking

The increasing usage of Smartphones has enabled individuals to use various applications including mobile banking applications. More and more individuals have started using mobile applications for banking as compared to the traditional desktop/Web-based banking applications.

Mobile banking refers to the use of a Smartphone or other cellular device to perform online banking tasks while away from your home computer for various uses such as monitoring account balances, viewing mini statement, account statement, transferring funds between accounts, bill payment etc.

Threats to Mobile Banking:

Mobile Banking Malwares:

There have been incidents that involved sophisticated virus infecting bank's mobile apps users to steal password details and even thwart two-factor authentication, by presenting victims with a fake version of the login screen when they access their legitimate banking application. A key vector by which the mobile banking malware get into the mobile device is through malicious applications posing as legitimate applications that users download and then become infected.

For prevention against Malware attacks:

- Download and use anti-malware protection for the mobile phone or tablet device.
- Keep the Banking App software up to date: Using the latest version of software allows receiving important stability and security fixes timely.
- Use security software: Applications for detecting and removing threats, including firewalls, virus and malware detection and intrusion-detection systems, mobile security solutions should be installed and activated.

- Reputed applications should only be download onto the smart phone from the market after look at the developer's name, reviews and star ratings and check the permissions that the application requests and ensuring that the requests match the features provided by that application.

Phishing Attack:

An attacker attempts phishing on to a mobile phone through SMS (Short Message Service), text message, telephone call, fax, voicemail etc. with a purpose to convince the recipients to share their sensitive or personal information.

For prevention against phishing attacks

- Emails or text messages asking the user to confirm or provide personal information (Debit/Credit/ATM pin, CVV, expiry date, passwords, etc.) should be ignored.
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) should be adequately implemented in mobile banking apps thus helping to prevent phishing and man-in-the-middle attacks.

Jailbroken or Rooted Devices:

This is practiced to gain unrestricted or administrative access to the device's entire file system, at the risk of exposing the device vulnerable to the malicious apps download by breaking its inherent security model and limitations, allowing mobile malware and rogue apps to infect the device and control critical functions such as SMS. Thus the mobile banking app security is exposed to extreme risk on a jailbroken device.

Outdated OSs and No Secure Network Connections:

Risk factors such as outdated operating system versions, use of no secure Wi-Fi network in mobile devices allow cybercriminals to exploit an existing online banking session to steal funds and credentials.

For prevention: Use Secure Network Connections: It's important to be connected only to the trusted networks. Avoid the use of public Wi-Fi networks. More secure and trusted WiFi connections identified as "WPA or WPA2" requiring strong passwords should be used.

Best Practices for Users to remain safe

- Enable Passwords On Devices: Strong passwords should be enabled on the user’s phones, tablets, and other mobile devices before mobile banking apps can be used. Additional layers of security inherently provided by these devices should be used.
- Bank account number or IPIN should not be stored on the user’s mobile phone.
- The user should report the loss of mobile phone to the bank for them to disable the user's IPIN and his access to the bank's account through Mobile Banking app.
- When downloading the Bank’s Mobile app in the mobile device, the user should go to a trusted source such as the App Store on the iPhone® and iPod touch® or Android Market. User can alternately check the Bank’s website for the details of the ways to receive App download URL, whether in the response to his SMS or email to the bank and then install the application. The app from any other third party source should not be downloaded.

Reference:

http://www.cert-in.org.in/

Secure Usage of Credit & Debit Card/ATM

Security Threats

Identity theft

The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories :

1. *Application fraud*

Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

2. *Account takeover*

Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent.

Credit card fraud

Credit card fraud is committed by making use of credit/debit card of others for obtaining goods orservices. The threat emerge due to stealing of information like Credit card number, PIN number,password etc. Theft of cards and cloning of cards are also employed to commit such frauds.

Hackers use complex techniques like Phishing, Skimming etc. to gain credit card information from innnocent users.

Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and creditcard details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can procure victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victim's credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card and makes note of card details for further use.

Vishing

It is one of the method of social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and "phishing".

Social Engineering

Social engineering involves gaining trust – hence the fraudster poses as a member of staff or even security guard. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of ATM machine and requires assistance.

Steps to be followed before Credit card & Debit card/ATM card usage :

- Whenever you receive the card from the bank make sure the mail is completely sealed and there is no damage.
- Whenever you receive the card from the bank immediately sign on the card.
- Try to cover the last three digit number on the card.
- Register your phone number to check the account transactions.
- Change the pin number immediately.

Secure usage of credit/Debit cards at Shopping malls and Restaurants

- Always keep an eye how the vendor swipe your card.
- Always make sure that the transactions happen at your presence.
- Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt.
- Don't give away your personal information in the survey forms given in restaurants/shopping malls.

Secure usage of credit / Debit card over internet

- Always use secure websites for transaction and shopping.
- Please look for signs of security.
- Identify security clues such as a lock image at the bottom of your browser, A URL that begins with http (These signs indicates that your purchases are secured with encryption to protect Your account information).
- Always shop with merchants you know and trusts.
- Always log off from any website after completing online transaction with your credit / debit card and delete the browser cookies
- Treat all e-mail messages with suspicion to avoid phishing scams. Do not respond to e-mail messages asking for personal information including financial information, as banks do not ask for such information.
- Never send payment information via e-mail. Information that travels over the Internet (such as e-mail) may not fully protected from being read by outside parties.
- Please be careful when providing personal information online.
- Please be wary of promotional scams. Identity thieves may use phony offers asking for your personal information.
- Please keep your passwords secret. Some online stores may require you to register with them via a username and password before buying. Online passwords should be kept secret from outside parties the same way you protect your ATM PIN.
- Always make sure to use the virtual keyboard for net banking.

Do’s

- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM.(to avoid skimming)
- Shield the ATM pin number during transaction. Don’t carry the transaction receipts along.
- Please change your ATM PIN once in every 3 months. As advised by banks.
- Keep your credit card receipts to guard against transaction frauds, check your receipts against your monthly statement.
- Only carry around credit cards that you absolutely need.
- Shred anything that contain your credit card number written on it. (bills)
- Notify your credit card issuers in advance of your change of address, then you change home address.
- If you lose your credit card, please report the loss immediately.
- When you dispose a card at the time of renewal/upgradation, please make sure to cut it diagonally before disposal.

Don’ts

- Don’t accept the card received directly from bank in case if it is damaged or seal is open.
- Don't write your PIN number on your credit card.
- Don't carry around extra credit cards that you rarely use.
- Don’t disclose your Credit Card Number/ATM PIN to anyone.
- Don’t hand over the card to anyone, even if he/she claims to represent the Bank.
- Don’t get carried away by strangers who try to help you use the ATM machine.
- Don’t use the ATM machines if the device is not in good conditions.
- Don’t transfer or share your account details with unknown/non validated source.
- Don’t access Netbanking or make payment using your Credit/Debit card from shared or unprotected computers in public places.
- Don’t open unexpected e-mail attachments from unexpected sources or instant message download links. Delete suspicious e-mail immediately.

- Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Never give your credit card info out when you receive a phone call. (This is called Vishing)
- Don’t provide your credit card information on a website that is not a secure site.
- Don’t share any confidential information such as password, customer id, Debit card number, Pin CVV2, DOB to any email requests, even if the request is from government authorities like Income Tax department, RBI or any card association company like VISA or Master card.
- Don’t address or refer to your bank account problems or your account details and password on social networking site or blogs.
- Don’t store critical information like your ATM PIN number on your mobile phone.

*****Case Studies related to Credit and Debit Cards:**********

Credit Card Fraud Is Funding Terrorist Networks: Not Digital Gold Currency

By: Mark Herpel July 16,2008

For OpEdNews: DGCmagazine - Writer

We should be extremely concerned about the scope of the credit card fraud problem involving terrorists. There is limited or no empirical data to gauge the extent of the problem. However, there are compelling signs that an epidemic permeates. [1]

Recently, there has been a string of articles in the main steam media attempting to link Digital Gold Currency and terrorist financing. However, the reality of the situation is that no Digital Gold Currency has ever been connected to a terror financing case or crime. Last month, even one very visible government report on Digital Currency stated, *"Such emerging electronic payment systems are vulnerable to money laundering and terrorist financing."* [2]

As far back as January 2006, the main stream media began an effort to connect terrorist funding and Digital Gold Currency. This trend seems to have started when a BusinessWeek "investigative report", quoted some dialog from Mr. Phil Williams, a professor of international affairs at the University of Pittsburgh and consultant to the United Nations on terrorism financing.

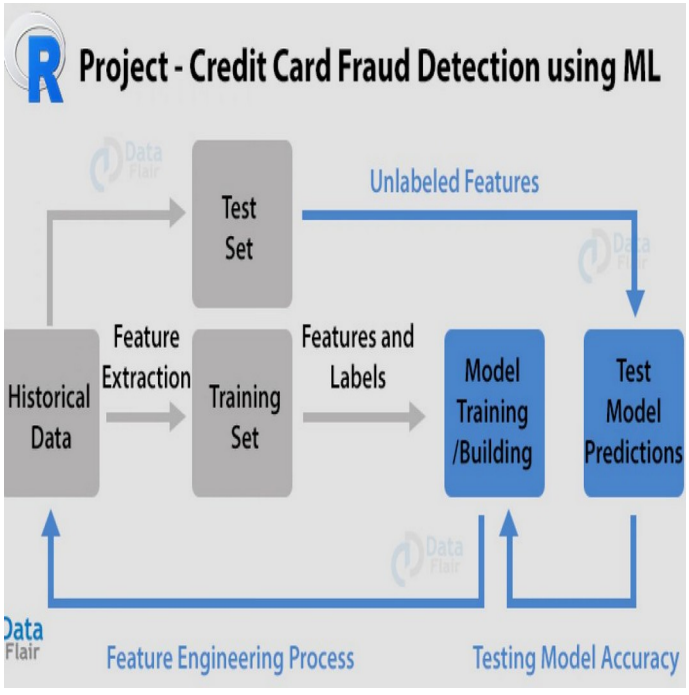
The article points out that while discussing digital currency, Mr. Williams says, *"At some point, this is going to be used" by terrorists.* Of course it is obvious from his comment that Mr. Williams has never seen the extensive Customer Verification Process required by GoldMoney, e-dinar or Crowne Gold. It is also doubtful that Mr. Williams has ever transacted an exchange of dollars into e-gold digital currency using a professional exchange agent.[3](Businessweek Article By Brian Grow, John Cady, Susann Rutledge, and David Polek)

Credit card fraud has become an ever present tool for funding terror networks while Digital Gold Currency has never even been mentioned during the prosecution of a terror crime. Look at the facts as far back as 2001.

Ii Al Marri was arrested in Illinois in December 2001 for having lied to FBI Agents about having contact with facilitators of the 9/11 terrorist attack. At the time of arrest, Al Marri had 36 credit card numbers and account information in his possession. A subsequent search of his computer found he had compiled over 1,000 credit card numbers and other identifying information. [4]

Doesn't "The truth" still have a place in main stream media? Isn't it important to discuss the facts as received directly from law enforcement professionals and not the suspicions and gossip of investigative reporters?

Complaint: I have been using the services of First Abu Dhabi Bank (FAB) credit card for some time now. Recently, my card was used more than five times for fraudulent transactions. I got in touch with the bank's customer care and blocked the card immediately. The bank executive advised me to send the dispute form, which I did.



Online Payments through

Unified Payment Interface (UPI)

Unified Payment Interface (UPI) is an initiative by National Payments Corporation of India (NPCI), set up with the support of the Reserve Bank of India with a vision of migrating towards a "less-cash" and more digital society. UPI is a system that enables peer to peer online payments for users holding different bank accounts, to send and receive money or to pay directly to merchants from their Smartphone without the need to enter bank account information or net banking UserID / Password. UPI has built on the Immediate Payment Service (IMPS) platform.

How it works

For using Unified Payment Interface, users need to create a Virtual ID or Virtual Payment Address (VPA) of their choice to link it to any bank account. This process doesn't require either the payee or payer to share bank details. The VPA acts as their financial address and users need not remember beneficiary account number, IFSC codes or net banking user id/password for sending or receiving money.

Steps for Registration:

- User downloads the Unified Payment Interface application from the App Store / Banks website.
- User creates his/ her profile by entering details like name, virtual id (payment address), password etc.
- User goes to "Add / Link / Manage Bank Account" option and links the bank and account number with the virtual id.

Generating M-PIN:

- User selects the bank account from which he/she wants to initiate the transaction.
- User clicks on the given options as required.

Performing a Unified Payment Interface Transaction

PUSH-sending money using virtual address

- User logs in to UPI application.
- After successful login, user selects the option of Send Money / Payment.
- User enters beneficiary's / Payee virtual id, amount and selects account to be debited.

- User gets confirmation screen to review the payment details and clicks on Confirm.
- User now enters MPIN.
- User gets successful or failure message.

PULL-Requesting money

1. User logs in to his bank's UPI application.
2. After successful login, user selects the option of collect money (request for payment).
3. User enters remitters / payers virtual id, amount and account to be credited.
4. User gets confirmation screen to review the payment details and clicks on confirm.
5. The payer will get the notification on his mobile for request money.
6. Payer now clicks on the notification and opens his banks UPI app where he reviews payment request.
7. Payer then decides to click on accept or decline.
8. In case of accept payment, payer will enter MPIN to authorize the transaction.
9. Transaction complete, payer gets successful or decline transaction notification.
10. Payee / requester get notification and SMS from bank for credit of his bank account.

Advantages

- With UPI, user's bank account can be used as a wallet with a simplified two-factor authentication which eliminates the need to store funds in any other wallet.
- Use of Virtual ID makes it more secure since there is no need to share credentials.
- UPI transaction can be made via IMPS in real time, which makes it available 24*7.
- Users can link multiple bank accounts to a single Smartphone. Hence sending or receiving money across banks is easier.
- For merchants, it is Suitable for electronic Commerce and a mobile Commerce transaction as well as it resolves the Cash on Delivery collection problem.
- Banks can create their own application interfaces as UPI provides flexibility and an open architecture.

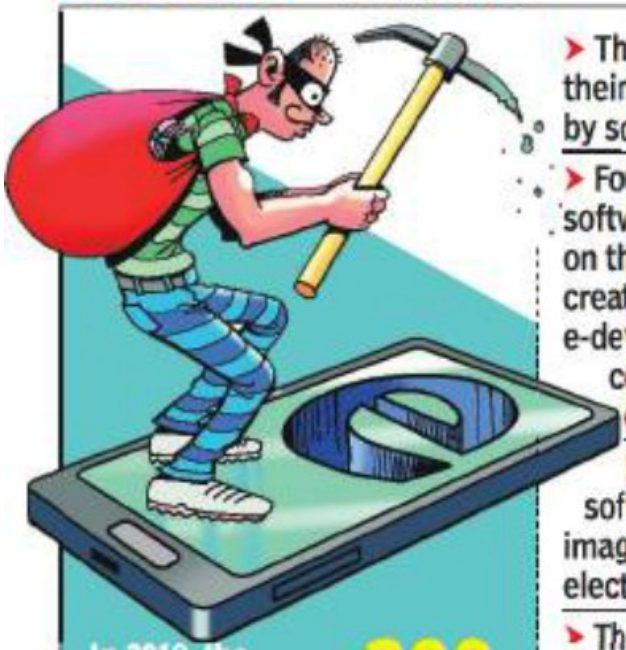
Security Measures

1. Beware of Mobile phishing: always download legitimate UPI applications from bank's official website, and be cautious before you download it from App store.
2. Keep strong passwords for your phone as well as for your UPI application.
3. Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank.
4. Use biometric authentication if possible.
5. Update your mobile OS and applications as often as possible to be secure from vulnerabilities.
6. It is advisable for users to enable encryption, remote wipe abilities and anti-virus software on the phone.
7. Keep your SIM card locked with a Pin to avoid misuse, in case of loss or theft of the mobile device, You can contact your subscriber to block the subscription of the SIM card.
8. Avoid connecting phones to unsecured wireless networks that do not need passwords to access.
9.
10.
11.
12.
13.
14.

15.

****Case Studies related to UPI:**********

CROOKS' TRICKS



In 2019, the city police received **300** complaints of people downloading links sent to them by strangers on their cellphones & being duped

- The fraudsters send SMSs to random phone numbers, promising a reward for downloading a link
- Once the link is downloaded, the fraudsters gain remote access to the targets' devices
- The targets do not realize their devices being accessed by somebody
- Four to five types of software are available on the internet, which create the mirror images of e-devices, such as laptops, cellphones and desktops, connected to the internet
- The fraudsters use these software to create the mirror images of their targets' electronic devices
- They then transfer money from the targets' UPI-linked bank account to another bank account
- They also make online purchases on various e-commerce websites
- Complaints with the cybercrime police reveal that the targets have been cheated in between ₹4,000 and ₹2 lakh after they clicked on the suspicious links shared through the text messages

UPI hits 1 bn transactions in Oct, plans to go global

Mumbai: Transactions using India's own domestic payments platform — Unified Payments Interface (UPI) — hit a landmark of one billion in September, three years after its launch.

UPI also recently crossed 100 million users, making it the fastest adoption of any payments system anywhere in the world.

Having achieved this double milestone, the National Payments Corporation of India (NPCI), which operates the UPI platform, aims to take the network global by enabling acceptance of UPI in Singapore and the UAE.

The UPI platform, which was launched before demonetisation in 2016, enables users to send money from their account to any account without entering bank details by using an email-like handle or scanning a QR code. The NPCI, which launched the RuPay network, had launched this to promote digital payments by harnessing the ubiquitousness of smartphones.

"The UPI has had the fastest acceptance not just in payments but among other platforms as well. I have not compared the numbers but given the time taken to reach 100 million users by social media and other platforms, I am sure we should be among the top," said Dilip Asbe, chief executive officer, NPCI. To put things in perspective, in August the total volume of all card transactions (debit and credit) put together was 142 crore (1.42 billion).

While all major banks are part of the UPI network and many have proprietary apps, the open architecture of UPI enables any bank account to be accessed from any UPI app.

▶ Fintech valuations, P 7

Valuations of fintechs push UPI volumes

▶ Continued from P 1

This has enabled three players—GooglePay, Paytm and PhonePe—to dominate the market as customers of different banks use largely these three apps and the NPCI's BHIM app to transact. These three have been the most aggressive in enrolling small merchants, including hawkers, to accept payments through the UPI. What has also helped is that UPI waived merchant fees for payments up to Rs 100.

The foreign investor backed fintechs that have been driving UPI volumes have gained in terms of valuations, given the market potential. Walmart-owned PhonePe, according to a Morgan Stanley report, is now worth $7 billion. Paytm has also seen its valuation soar in line with an in-

Bengaluru: Woman orders Rs 800 kurta, loses Rs 80,000

Kiran Parashar | TNN | Updated: Nov 26, 2019, 12:52 IST

RBI spots fraud that wipes out a customer's bank balance via UPI, alarm sounded

Fraudsters get victims to download the AnyDesk app, which gives them remote access to the mobile. After that, all your OTPs are theirs too.

Vijay Shekhar ✓
@vijayshekhar

Pls don't trust any SMS send of blocking your Paytm account or suggestion to do a KYC.
These are fraudsters attempting on your account. Pls RT.

5:20 PM · Nov 19, 2019 · Twitter for iPhone

Doc's card swiped for ₹4L instead of ₹40 at toll booth

Mangaluru: A groggy toll attendant swiped Rs 4 lakh instead of Rs 40 from a doctor's debit card at Gundmi toll gate on the Kochi-Mumbai National Highway near Udupi around 10.30pm Saturday. The toll gate is 18kms from Udupi.

Remote-access apps used to steal money from a/c

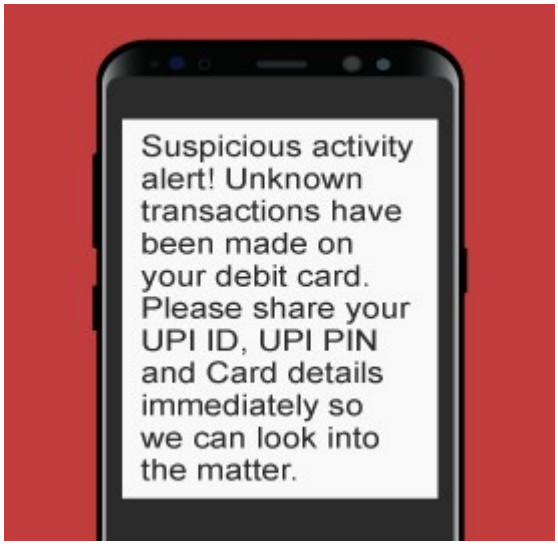
Mayur.Shetty
@timesgroup.com

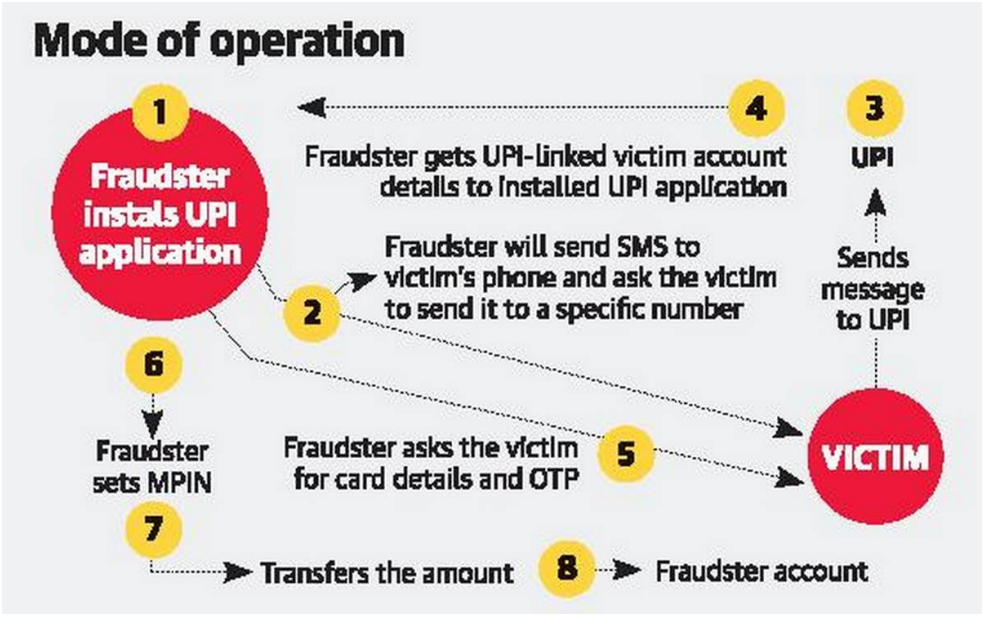
Mumbai: A new fraud has emerged where the customer is led to install a third-party app, which provides access to the bank account. A Bengaluru-based former bank official lost Rs 1 lakh after fraudsters gained access to his phone by getting him to download an app that allows for malicious access.

MALICIOUS USE OF UPI

bank's branch, he was informed that the money was transferred to an Aditya Birla Payments Bank account using the Unified Payments Interface (UPI) platform. While five transactions were made to withdraw Rs 1.24 lakh, the fraudsters were successful in debiting only Rs 1 lakh. However, Hegde received alerts for just two of the five transactions.

"Banks shouldn't make their clients run around and should follow the RBI guidelines to pay up customers when they fall prey to





Reference:

http://www.cert-in.org.in/