



Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

सी डैक
CDAC

CYBER SECURITY HANDBOOK FOR DIGITAL FINANCIAL TRANSACTIONS

Engineering E-Wallet Finance
PoS Transactions IT laws Digital payment
Skimmers Credit card Finance
Cash
UPI
AEPS USSD PHISHING
prepaid cards Payments
Mobile Banking Micro ATM SBIM



Ministry of Electronics and Information Technology (MeitY)
Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Sitaram Highway,
Pahad Sharief Via Keshavnagar (Post), Hyderabad - 501310, Telangana (India) | Nalanda Building, No. 1 Shreebagh Salyam Theatre Road,
Amberpet, Hyderabad - 500016, Telangana (India)



SECURE *

‘S’ for Security for citizens,
‘E’ for Economic development,
‘C’ for Connectivity in the region,
‘U’ for Unity,
‘R’ for Respect of sovereignty and integrity, and
‘E’ for Environment protection.

Shri Narendra Modi

Hon’ble Prime Minister
@Asian Summit SCO, Bats For ‘SECURE’

India’s Digital economy is on the high way of great growth and my department has taken a commitment that we will make India’s digital economy a one trillion dollar economy in the coming 5 to 7 years. When I talk about digital economy I mean communication, IT and IT enabled services , e-commerce, **cyber security** , digital payment and electronic manufacture

Shri Ravi Shankar Prasad

Hon’ble Union Minister Law and Justice and Electronics and Information Technology
Government of India



Reference* : <https://www.msn.com/en-in/sports/ipl-videos/pm-modi-at-asian-summit-sco-bats-for-secure/vp-AAyrwVr>

PREFACE

In today's digital world, most of the financial transactions, financial investments and holding of financial investments are held in electronic form and transacted through the cyber space taking over traditional banking/investing system. Majority of the population has moved to online methods of financial investments and transactions. Online means of investments to attain financial security are less expensive in terms of operational costs for both the bank and consumer, but they expose both banks and customer to a large number of cyber security risks. Considering the amount of confidential information held by a financial institution and the amount of financial transactions taking place on daily basis, cyber security risks in finance sector have to be taken care of with great significance.

The negative side of cyber world is both inevitable and unavoidable in the financial sector. It's the reality that cyber criminals are targeting financial institutions as well as individuals by taking advantage of vulnerabilities used in the financial applications and lack of awareness among the end users. We take special care and safety measures to protect our family and children from the social threats prone to them in the cyber world. Similarly, it is equally important to cyber secure your financial savings from cyber threats. Today we share our financial data in many places like online shopping, e-wallets, POS terminals, online ticket booking, hotel booking and many more without even knowing whether these places can provide security to your sensitive information or not. Therefore, it's our responsibility to protect and take care of our personal sensitive data.

The importance of cyber security in the current scenario of digital transformation going on India was identified and the initiation was taken by Ministry of Electronics and Information Technology (MeitY) which has approved a project titled Information Security Education and Awareness (ISEA). The main objective of this project is to spread awareness on Information security among people of India. Considering the relevance of digital payments where Indian economy is in the phase of moving towards cashless economy this cyber security handbook on 'Digital Financial Transactions' has great importance to impart awareness among people.

This handbook covers all the various digital transactions systems in India and the threats associated with them. It also gives an insight to the mitigation methods to stay safe in this digital world. Let us together take the first step of being aware of what can happen in digital world in terms of financial frauds; and to safeguard ourselves and our family.

Our Sincere Acknowledgements for the support provided by
Ministry of Electronics and Information Technology (MeitY), Government of India



CONTENTS

Page 5	Introduction Digital payment methods in India	Page 26	Point-Of-Sale Machines Introduction How to use Threats to Point-Of-Sale machines Best practices to stay safe for users
Page 8	Debit/Credits Cards Introduction How to use Threats to Banking cards Best practices to stay safe for users	Page 28	Micro ATMS Introduction How to use Threats to Mobile Banking Best practices to stay safe for users
Page 12	Unified Payment Interface Introduction How to use Threats to UPI Best practices to stay safe for user	Page 30	Online banking Introduction How to use Threats to Internet Banking Best practices to stay safe for users
Page 14	Bharat Interface for Money (BHIM) app Introduction How to use Threats to BHIM App Best practices to stay safe for users	Page 34	Mobile Banking Introduction How to use Threats to Mobile Banking Best practices to stay safe for users
Page 16	USSD Introduction How to use Threats to USSD Best practices to stay safe for users	Page 36	Cyber Laws in India Advantages of Cyber Laws Importance of IPC Frauds relating to computers
Page 20	Aadhaar Enabled Payment System (AEPS) Introduction How to use Threats to AEPS Best practices to stay safe for users	Page 46	Guidelines to report financial frauds in India If you find an unauthorized transac- tion on your account. How to file a cyber crime complaint in India Cyber cells in India IT laws
Page 22	E-Wallet Introduction How to use Threats to E-wallets Best practices to stay safe for users		

CREDITS



Ministry of Electronics
and Information Technology
Government of India

For Virus Alerts, Incident & Vulnerability Reporting



Shri.Sitaram Chamarthi (TCS)

Shri U Rammohan Rao, CID,
Telangana State

Shri G V Raghunathan,
(Retd) Sr Director, MeitY

Shri Magesh E, Director,
C-DAC Hyderabad

Shri S K Vyas, MeitY

Shri Ch A S Murty
Mrs Soumya M
Mrs Indrakeerthi K &
ISEA Team Members,
C-DAC Hyderabad

Honorary Professor. N Balakrishnan
Prof. Sukumar Nandi
Prof. V Kamakoti
Prof. M S Gaur

Action Group Members

A K Piplal, HoD (HRD), MeitY
Shri.Sitaram Chamarthi
Prof. M S Gaur
Prof. Dr.Dhiren R Patel
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasara Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, Additional Director,
MeitY



Message from

E Magesh

Director, C-DAC Hyderabad

Securing your hard earned money is a prime task to everyone.

With the bloom of digitalization in India, there has been manifold increase in the digital transactions in India by touching almost one lakh crore rupees a month. At the same time there is a significant jump in the number of financial frauds and the value, making it a major concern to the people in India and elsewhere.

Each day fraudsters devise new methods to execute frauds. Financial fraud both online and offline can impact the individual with direct financial loss leading to emotional and psychological stress. The current edition of handbook will help the readers to understand the complete scenario of financial frauds and how to secure your money. With the advent of low-cost Internet services, it can be seen that the more number of the population accessing online services more proactively.

Most of the Physical money transactions are replaced by online transactions. With this there is a need to raise awareness among people on the types of financial frauds and methods employed by fraudsters to commit fraud. C-DAC Hyderabad, being the coordinating center for creating mass awareness on Information Security under the purview of ISEA Project Phase II, is glad to release this handbook on such an important topic, which is of interest for most of the stake holders.



Introduction

Indian economy is undergoing a transformation through 'Digital India', the flagship programme of Government of India to create a digitally empowered society and knowledge economy. To achieve the dream of cashless economy, it is important that all sections of the society be aware of various methods of financial transactions and also gets equal opportunity and participates in nation building. Government of India has taken measures to promote a cashless economy through digital payments.

Government has supported by introducing various online methods of payments like Aadhaar Enabled Payment System (AEPS), Bharat Interface for Money (BHIM), Immediate Payment Service (IMPS), Unified payment Interface (UPI), PoS machines etc. India has shown a tremendous progress in banking methodologies from traditional banking to Electronic

banking followed by use of credit cards. Current decade is witnessing a popularization for digital payments like electronic wallets, swipe cards, debit cards, cardless payment methods etc. We need to take a leap forward towards achieving the dream of Digital India and cashless economy.

Lack of awareness on digital financial literacy, especially among the rural population is a major challenge for the country. Digital methods of financial services are a major target for cyber criminals. The Debit/Credit cards, Net Banking solutions and even the transaction websites of the financial institutions and banks are hacked by the cyber criminals. This has led to an urgent need to create awareness among the citizens, especially in rural and semi-urban areas regarding digital finance services and also enable/support them to access various digital finance

services, details about the government policies, the various threats which they may face while using these digital services and also about the various mitigation methods to be safe while using digital payment services. In view of this Ministry of Electronics and Information Technology (MeitY) has approved a project entitled Information Security Education and Awareness (ISEA). In the present scenario where in the life of an individual, technology plays a vital role, it is better to be aware on how to detect, how to protect and how to recover from cyber threats in financial sector?

In this handbook we give an insight to the (i) Different types of Digital Payment methods in India, (ii) How to Use those Digital Payment methods (iii) What are the various threats in these methods (iv) Different mitigation methods to stay safe (v) Guidelines to report financial fraud in India.



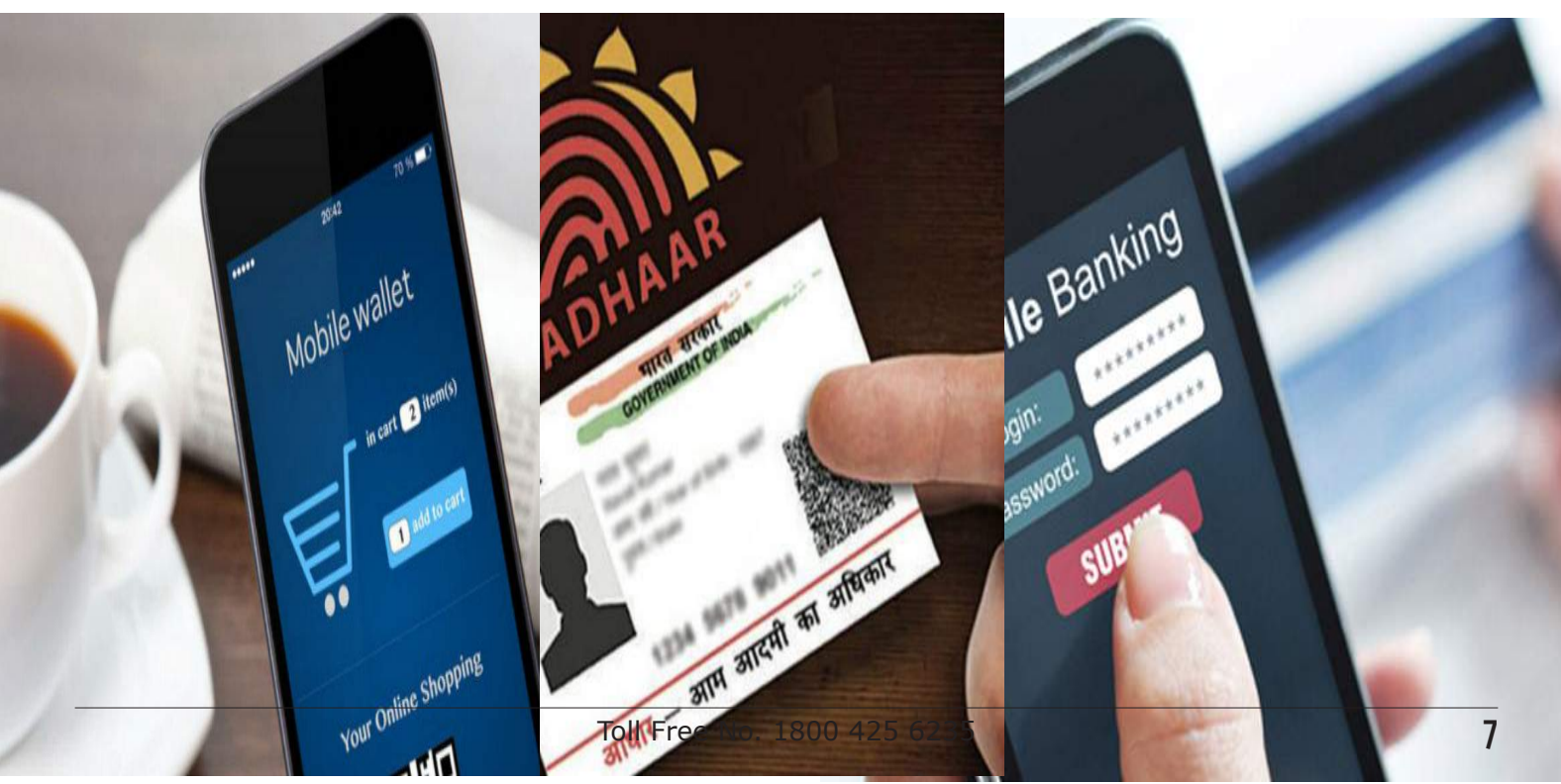
Digital payment methods in India

A digital transaction is a seamless system, where transactions are effected without the need for Physical cash. To use digital payment methods, the user will have an existing bank account which they own and should have available funds in their accounts to make cash payments or to receive revenue via digital platforms including mobile devices, personal computers or the internet. Ideally digital payment

systems will have three key components of any such digital financial services: a digital transactional platform, retail agents, and the use by customers and agents of a device, usually a mobile phone, to transact via the platform.

Banks, microfinance institutions, mobile operators, and third party providers are leveraging mobile phones, point-of-sale devices, along with networks of small-scale

agents, to offer basic financial services at greater convenience, scale and lower cost than traditional banking allows. The major types of Digital payment Methods are as follows: Banking Cards, USSD, Aadhaar Enabled Payment System (AePS), Unified Payment Interface (UPI), E-Wallet, bank pre paid cards, Point-Of-Sale, Internet banking, Mobile Banking, Bharat Interface for Money (BHIM) app.





DEBIT/CREDIT CARDS

What are the different types of cards?

There are three types of cards: Debit cards, Credit cards and prepaid cards.

Debit Cards:

Issued by the Bank where you have an account. It is linked to the bank account. User can use this card to withdraw cash up to the limit present in his/her bank account. It can also be used only for domestic fund transfer from one person to another.

Credit Cards:

Issued by banks / other entities approved by RBI. Unlike debit cards, in case of credit cards, a customer can also withdraw beyond the amount

of money present in his bank account. But there is a limit for each credit card up to which extra money can be withdrawn. Also there is a time limit and interest charges to be paid back.

Prepaid Cards:

These are pre-loaded from a customer's bank account. It can be used for limited amount of transaction. These can be recharged like mobile recharge and are very safe to use. The main advantage of debit/credit or prepaid banking cards is that they can be used to make other types of digital payments. Some of the most reputed and

Cards are among the most widely used payment methods and come with various features and benefits such as security of payments, convenience, etc. These are usually issued by banks and can be classified on the basis of their issuance, usage and payment by the card holder.

well-known card payment systems are Visa, Rupay and MasterCard, among others. Banking cards can be used for online purchases, in digital payment apps, ATM machines, PoS machines, online transactions, etc.

Apply with your respective bank and provide Know Your Customer (KYC) details his respective bank branch. Debit cards can be exchanged with Rupay Card. Bank account is mandatory to get the card. As per Government orders, all the Jhan Dhan account holders will be issued Rupay Cards.

How to use Debit/Credit Cards ?

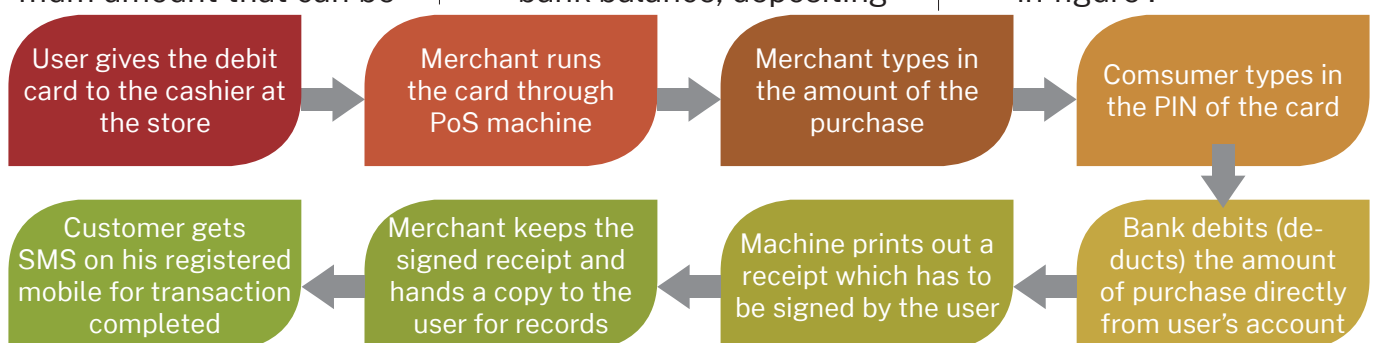
- To withdraw money from an ATM, user needs to insert his/her debit/credit card and type in your unique PIN Number (4 digits) which is provided by the bank. The maximum amount that can be

withdrawn per day is set by the bank.

- With debit card, user can also use the ATM to carry out other financial and nonfinancial transactions such as finding out bank balance, depositing

cheque or money, getting a mini statement, etc. without visiting the bank branch.

- While shopping at major retail stores and shops, follow the process shown in figure :



Online Transactions using Debit / Credit cards

Individuals have started opting for social media and mobile apps for most of the banking transaction. There are three different ways like RTGS, NEFT and IMPS through which we can transfer funds from one bank account to another.

NEFT is an electronic fund transfer system which operates on a DNS (Deferred Net Settlement) basis which settles transactions in batches. You can use the NEFT service through the bank branch through cheques, DD or you can make the transfer using net banking facility in your bank account. There is no mini-




mum limit on the amount that can be transferred.

RTGS : In RTGS the transactions are settled individually and not in batches. The transaction is processed immediately after it is executed throughout the RTGS business hours. The RTGS window is open from 8 am to 4 pm between Monday and Saturday except 2nd and 4th Saturday as well as bank holidays. The minimum limit on transfer of funds at a time is Rs 2 lakhs.

IMPS : It is an instant payment service available for money transfer to bank accounts in India. It is ideal for transactions

with small amount. The main feature of IMPS service is that it is available 24/7 including Sunday and bank holidays throughout the year, which makes it particularly helpful during emergencies. IMPS is basically used for transfers using the mobile phone number through apps or mobile banking. You can also use IMPS in your netbanking services for when you want to transfer using account number details. The process is the same as NEFT. There is a limit of Rs 2 lakhs if you use the online transfer using bank account in netbanking.

Steps to protect from financial fraud through credit card

-  Always keep your payment transaction applications updated with latest version
-  Always keep an eye on your card during usage and promptly take it back
-  Always check if there is any discrepancy between transaction SMS details and actual transaction



Threats to Debit / Credit cards

Credit/debit card fraud

Credit card fraud is committed by making use of credit/debit card of others for obtaining goods or services. The threat emerges 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 innocent users.



Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity through e-mail. Phishing is typically carried out by e-mail spoofing 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.



Best practices for users to remain safe

- Do not share your card information over the phone or internet with ANYONE, irrespective of whether you know them or not.
- Do not give any card or personal information while answering a telephone call where the caller claims to represent the card issuing bank or any related organization. You can always call back the bank on publicly displayed numbers, if required.
- While making payment at a merchant location or service provider like restaurants, etc, insist on punching in your PIN rather than hand over your card for processing the payment.
- Always check the bill.
- Always retain the transaction receipt for comparing against the card statement that you receive at the end of the month. Most people throw this away and do not match against the amount charged in the statement.
- Do not throw away the transaction receipt when you are done with it. Tear it or shred it. Dumpster divers are known to sift through garbage bags meticulously and retrieve all your card related information that can then be used to conduct unauthorized purchases, especially over the internet.
- While using an ATM, ensure that no one is watching your finger movement as you type your PIN. Watch out for cameras within the premises that can easily capture your PIN number. Try and cover your hand while you type in the PIN.
- Always memorize your card and PIN numbers, and in case of any loss or theft, report immediately to the concerned bank so that they can temporarily freeze your account and prevent any further unauthorized transaction until you receive your card replacement.
- Never save your card password in a regular folder in your computer hard drive or email account. If the account gets hacked, there is every possibility that an unauthorized transaction will take place.
- While making a payment over the internet, check for the security logo on the website confirming it as a safe site. If in doubt, check with the concerned company before making any such payment.
- Avoid keeping your credit or debit card in the wallet. In case your wallet gets stolen, you will at least have access to money at that moment.
- Download banking apps directly from the bank website and avoid using links that you receive via email or SMS to download your banking app.
- As card users, have to do your part towards securing your hard earned money, while the banks need to work harder towards securing information and money.





UNIFIED PAYMENT INTERFACE (UPI)

Today UPI is the best way to digital payments. People want to know the use of UPI in SBI Pay, Paytm, Phonepe, Tez and other apps. In fact, all these apps are riding on UPI wave. After the launch of UPI, the mobile app payment has setback.

UPI is a type of interoperable payment system through which any customer holding any bank account can send and receive money through a UPI-based app. The service allows a user to link more than one bank account on a UPI app on their smart phone to seamlessly initiate fund transfers and make collect requests on a 24/7 basis and on all 365 days a year. The main advantage of UPI is that it enables users to transfer money without a bank account or IFSC code. All you need is a Virtual Payment Address (VPA). There are many UPI apps in the market and it is available on both Android and iOS platforms. To use the service one should have a valid bank account and a registered mobile number, which is linked to the same bank account. There are no transaction charges for using UPI. Through this, a customer can send and receive money and make balance enquiries.

How to use UPI ?

To use the UPI payment system we need a mobile app. The app communicates with the UPI system and facilitates the fund transfer. But to keep the whole system secure, a bank has to play the role of intermediary. That is why every UPI app must be sponsored by a bank. Every participating bank of UPI can sponsor or make many apps. The banks have made their own UPI based app

such as SBI Pay, Baroda Pay, iMobile etc. On the other hand, they have also sponsored the apps of some other companies such as Yes Bank is sponsoring Phonepe, ICICI Bank and SBI is sponsoring Tez.

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

1

User downloads the Unified Payment Interface application from the App Store / Banks website.

2

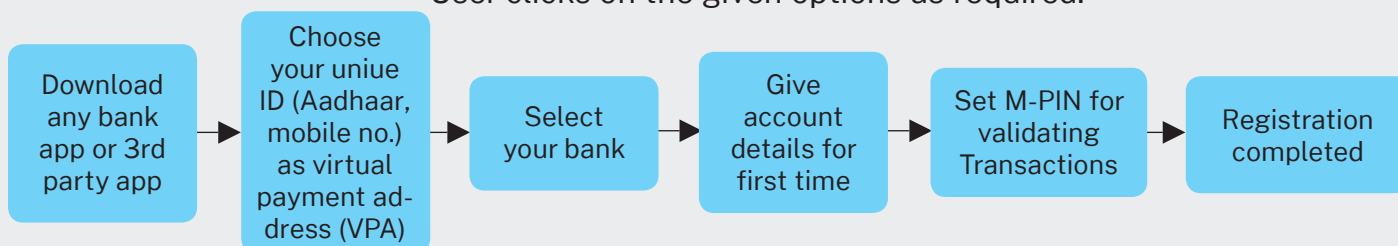
User creates his/ her profile by entering details like name, virtual id (payment address), password etc.

3

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

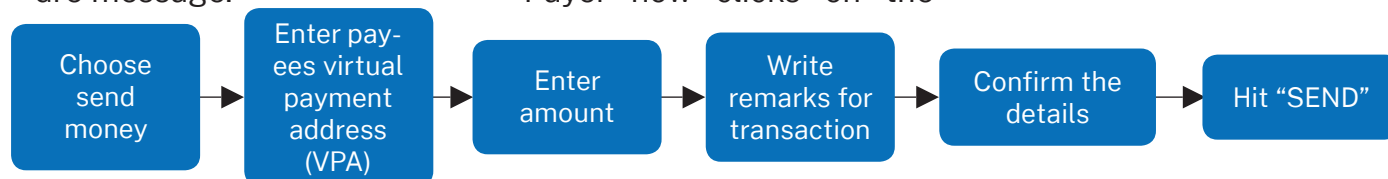
- User logs in to UPI application.
- After successful login, user selects the option of Send Money / Payment.
- User enters beneficiary's / Payee virtual id, amount and selects account to be debited.
- User gets confirmation screen to review the payment details and clicks on Confirm.
- User now enters MPIN.
- User gets successful or failure message.

PULL-Requesting money

- User logs in to his bank's UPI application.
- After successful login, user selects the option of collect money (request for payment).
- User enters remitters / payers virtual id, amount and account to be credited.
- User gets confirmation screen to review the payment details and clicks on confirm.
- The payer will get the notification on his mobile for request money.
- Payer now clicks on the

notification and opens his banks UPI app where he reviews payment request.

- Payer then decides to click on accept or decline.
- In case of accept payment, payer will enter MPIN to authorize the transaction.
- Transaction complete, payer gets successful or decline transaction notification.
- Payee / requester get notification and SMS from bank for credit of his bank account.



Best Practices for Users to remain safe

- Beware of Mobile phishing: always download legitimate UPI applications from bank's official website, and be cautious before you download it from App store.
- Keep strong passwords for your phone as well as for your UPI application.
- Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank.
- Use biometric authentication if possible.
- Update your mobile OS and applications as often as possible to be secure from vulnerabilities.
- It is advisable for users to enable encryption, remote wipe abilities and anti-virus software on the phone.
- 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.
- Avoid connecting phones to unsecured wireless networks that do not need passwords to access.

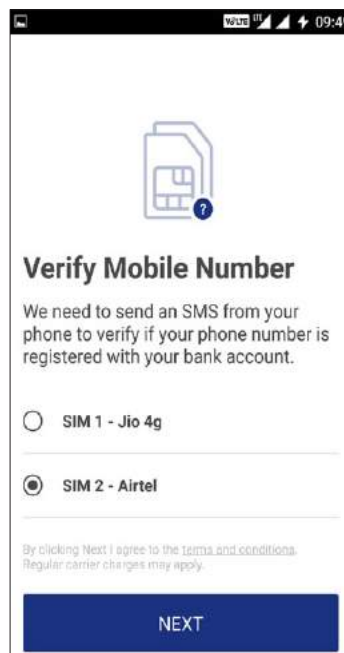
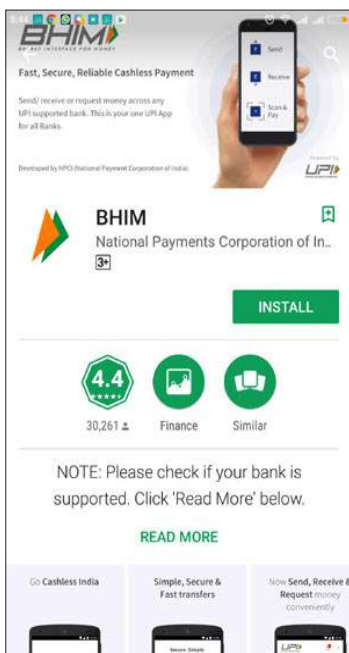


The BHIM app allows users to make payments using the UPI application. This also works in collaboration with UPI and transactions can be carried out using a VPA. One can link his/her bank account with the BHIM interface easily. It is also possible to link multiple bank accounts. The BHIM app can be used by anyone who has a mobile number, debit card and a valid bank account. Money can be sent to different bank accounts, virtual addresses or to an Aadhaar number. There are also many banks that have collaborated with the NPCI and BHIM to allow customers to use this interface.

BHARAT INTERFACE FOR MONEY (BHIM) APP

How to use BHIM App ?

- 1 Download and install the BHIM app
- 2 Choose a language
- 3 Register for the service by providing mobile number linked to bank account
- 4 Add bank-related information and set up a UPI PIN by following the given instructions





Send money

The option is simple to use. Tap on it > enter the phone number of the person who is going to receive the money. The number will be verified and if a UPI/BHIM account has been set up for that number, the app will accept the number and will take you to the next screen where you can put in the money and send it. If there is no number or UPI ID, you can also send the money using Bank Account + IFSC code. To access this option, click on three dots (settings) on the send money page.

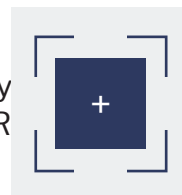


Request money

Again, tap on the request button. Put in the number, let the app verify it. Once the verification is done, you can request the money.

Scan and pay

This is the place where QR codes come into picture. The app generates a QR for every user, which can then be shared or printed and pasted. To make a payment to the QR code owner, just scan it and pay.



Threats to BHIM app

SQL injection vulnerability

SQL stands for Structured Query Language, used to communicate with a database. The code is written using SQL inline method, which is largely considered an insecure way of storing data.

Denial of services' attack

Hackers flood servers with fake transactions to bring them down. The app allows a user to have sender and receiver's account as the same, which means one can continue to send small amounts of

money to his or her own account, without making any real transaction but in the process, possibly clogging the system if other controls are not in place--something that may lead to a Denial of Service attack.

Best practices for users to remain safe

The steps to be taken care to protect yourselves from financial fraud through BHIM App.

- 1 Check the payment collect request details with the merchant before making the payment
- 2 Be sure to keep UPI based Apps updated.
- 3 Make sure you transfer money only to known beneficiaries.



UNSTRUCTURED SUPPLEMENTARY SERVICE DATA

Another type of digital payment method, *99#, can be used to carry out mobile transactions without downloading any app. These types of payments can also be made with no mobile data facility. This facility is backed by the USSD along with the National Payments Corporation of India (NPCI). The main aim of this type of digital payment service is to create an environment of inclusion among the underserved sections of society and integrate them into mainstream banking. This service can be used to initiate fund transfers, get a look at bank statements and make balance queries. Another advantage of this type of payment system is that it is also available in Hindi. However, this payment method can be used only for small value transactions up to Rs 5000 as per RBI guidelines.

In USSD, direct communication between sender and recipients is established and this promotes faster data transmission. USSD communication is session-oriented and it is easily implementable while being more user-friendly. The developer community prefers USSD channels for development of mobile payment application because of these powerful features.

How to use USSD ?

- 1 Provide KYC (Know Your Customer) information to open a new account
- 2 Mobile no. should be linked with bank a/c
- 3 Register for USSD/Mobile Banking
- 4 Get MMID (Mobile Money Identifier)
- 4 Get MPIN (Mobile PIN)

Services Offered

- 1 The various services offered are Balance enquiry, Mini Statement, Funds transfer, MMID, A/c no., Aadhaar, Know MMID, Change M-PIN, Generate OTP.

USSD

Select Option: (HDFC Bank)

- 1.Account Balance
- 2.Mini Stmt
- 3.Send Money Using MMID
- 4.Send Money Using IFSC
- 6.Show MMID
- 7.Change MPIN

1

CANCEL SEND

How to use USSD ?

- 1 This service can be used by dialling *99#, after which the customer can interact with an interactive voice menu through their mobile screen.



A screenshot of a USSD menu displayed on a mobile screen. The title bar is blue with the text 'USSD'. The main content area is white and contains the text: 'Welcome to *99#', 'Type 3 Letters of Bank Short Name OR', 'First 4 Letters of Bank IFSC OR', and '2 Digit Bank Numeric Code of *99#'. Below this text is a green input field with the placeholder text 'HDF'. At the bottom of the screen are two buttons: 'CANCEL' and 'SEND'.

- 2 To use the service the mobile number of the customer should be the same as the one linked to the bank account Register for USSD/Mobile Banking
- 3 The next step is to register for USSD, MMID (Mobile Number Identifier) and MPIN

Transaction Cost

- 1 NIL by system
- 2 Rs. 0.50 charged to customer

Threats to USSD

As previously mentioned, each bank has a unique short-code, but this is also backed by unique infrastructure. In fact, nearly all mobile financial service providers (banks, mobile money operators and payment service suppliers, etc.) operate unique applications in providing USSD services to customers. Therefore, it is possible that the risk exposure of USSD transactions increases because each financial service provider uses its own technology, meaning there is no universal standard for all channels.

More importantly, messages over USSD channels are not encrypted, leaving them vulnerable to being hacked.

- **USSD Commands Request/Response Tampering**

A malicious user can tamper with USSD command

requests and responses. This may cause confusion for the legitimate user and can also lead to fraudulent transactions. This request and response tampering is possible through hardware and software interceptors. Weak encrypted request and response messages are prime concerns in such threat vectors.

- **USSD Request/Response Message Replay Attacks**

When a phone is lost, an adversary may perform fraudulent transactions through an installed USSD application. An application must authenticate USSD request originator (authentication through combination of MSISDN, IMEI, PIN and unique Message Tracking ID). If this USSD application server

or application is unable to authenticate the USSD request originator, then it can perform fraudulent transactions.

- **USSD Server Response Tests**

The USSD application server should respond properly upon valid requests generated by an authenticated user. Weak encrypted response message, response delay and response exception handling (in case of buffer overrun, delivery notification) are the prime concerns in USSD application server response mechanism.





- **USSD Content Error Tests**

Improper USSD content error-handling may reveal sensitive information about customer data, USSD application and the service provider's sensitive data.

- **USSD Response Time Tests**

Improper USSD response time implementation may result in delay or tampering delivery notifications,

transaction success messages and alerts.

- **Verify Strong Cryptographic Implementation**

Weak cryptography implementation for critical data (customer number, card numbers, PIN, beneficiary details – account numbers, balance summary) can be tampered with, leading to fraudulent transactions.

- **Improper Session Management**

In this case, an adversary gets physical access to a victim's phone which has a USSD application installed on it. The adversary may perform any malicious activity on financial transaction modules (e.g. send money) due to improper session time-out implementation. It is also applicable to all financial transactions modules

Best practices for users to remain safe

Avoid the following for a safe and successful USSD banking :

- Do not reveal your PIN or BVN to a third party.
- Do not repeat a transaction delayed or interrupted by the network. This is because the transaction might have been processed. If you repeat such transaction your account might be debited twice. All you need do is to wait for an hour or more

for a notification on such transaction.

- Your phone should be charged to avoid loss of power in the midst of the transaction.
- Double-check the receiver's account number when transferring funds or paying bill. You must wait for the confirmation text from the bank that the transaction is successful.

- In absence of such confirmation and your account is debited, contact your bank immediately to resolve the transaction.
- In case of transfer, call the receiver to confirm receipt of the fund. If the response is no and your account has been debited, contact your bank to resolve it immediately.

Mitigation against Mobile Application and Operating System Attacks

- ☐ Update the mobile operating system regularly.
- ☐ Upgrade the operating system to its latest version.
- ☐ Always install applications from trusted sources.
- ☐ Consider installing security software from a reputable provider and update them regularly.
- ☐ Always check the features before downloading an application. Some applications may use your personal data.
- ☐ Do a good research about the application and the developer when you are downloading the application from third party.





SECURE USAGE OF CREDIT / DEBIT CARD



After receiving the card from the bank make sure the mail is completely sealed and there is no damage and immediately sign on the card

Ensure that your transaction is ended/completed at ATM machine before leaving the premise



Change the default pin number and don't forget to change it frequently



Do not respond to e-mail's asking for personal information including financial information, banks never ask for such information



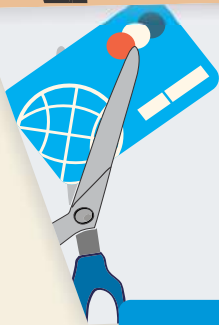
Monitor your credit card account statement regularly for suspicious / unauthorized activity

Before you use an ATM ensure that there are no strange objects in the insertion panel of the card



Always keep an eye on how the vendor swipes your card and make sure that the transactions happen at your presence

Never keep your credit / debit card and the PIN at one place



When you dispose a card for renewal/up gradation, please make sure to cut it diagonally before disposal

Always log off from any website after completing online transaction with your credit / debit card and delete the browser cookies



For more details / queries on Cyber Security visit or call us to our Toll free number



AADHAAR ENABLED PAYMENT SYSTEM (AePS)



How to use AePS

It is very simple to use AePs, all you need to do is to provide the accurate Aadhaar number and the payment will be successfully made to the concerned merchant. While using AePS do balance check of your Account, Aadhaar to Aadhaar fund transfer, Cash withdrawal, Cash deposit, Purchase at Fair Price Shops with AePS.

- Go to a micro ATM or banking correspondent
- Provide Aadhaar number and bank name
- Choose the type of transaction you want to make
- Provide verification through fingerprint/iris scan
- Collect your receipt

A customer will have to register his/her Aadhaar number to their existing bank account, provided their bank is AePS enabled. Through AEPS, the customer can withdraw or deposit cash, make the balance enquiry, and transfer funds. The maximum amount of transaction per account per day is Rs.50, 000.



Expanded as Aadhaar Enabled Payment System, AePS, can be used for all banking transactions such as balance enquiry, cash withdrawal, cash deposit, payment transactions, Aadhaar to Aadhaar fund transfers, etc.

It uses the Aadhaar number and biometric fingerprint of the user. AePS financial transactions are performed using Aadhaar enabled POS machines. AePS does not require any OTP or PIN for verification. It depends on data available with the UIDAI CIDR repository, which holds your authenticated data during the Aadhaar enrolment process. AePS performs payment transactions using the Bank Account linked with the Aadhaar Number of the user.

All transactions are carried out through a banking correspondent based on Aadhaar verification. There is no need to physically visit a branch, provide debit or credit cards, or even make a signature on a document. This service can only be availed if your Aadhaar number is registered with the bank where you hold an account. This is another initiative taken by the NPCI to promote digital payments in the country.

Threats to AePS

- Aadhaar enabled payments are built on a platform, which is Aadhaar. If any vulnerability affects Aadhaar, then Aadhaar enabled payments a payment system which is built on Aadhaar, will also be vulnerable and you may lose money.
- The Aadhaar Based Payment Systems may be vulnerable to the gummy finger method. Using gummy finger method your duplicate fingerprint can be made, just by using gum/glue. Fraudsters can make a transaction using your fingerprints and you can lose money. Cloning a debit/credit card is not very easy, but the gummy finger method where you need just gum/glue, makes Aadhaar Based Payment Systems vulnerable to fraud.
- The merchant uses the Aadhaar enabled payment system, to authenticate your fingerprints. Your biometric data could be stored on this device or the merchant can store your biometric data on his smart phone. This makes you vulnerable to fraud

Best practices for users to remain safe

- Always verify Aadhaar number before transferring money.
- Use a Aadhaar ID to carryout transactions only at POS and biometric data capture device.
- Ensure that the devices (POS and Biometric capture machine) are not tampered with only certified devices are being used.
- To secure the biometric data from unauthorized or malicious users who may attempt to access your customers' private and critical information or manipulate sensitive data to suit their goals to protect financial transactions from fraudsters

AePS gives a lot of convenience to the rural people. It brings the bank to their doorstep and saves much time and transport expense. It would be just like a visit of the ATM at every doorstep. That is why government calls the POS as micro ATM.





E-WALLET



An Electronic-wallet(e-wallet) is an electronic application that enables online e-commerce transactions like purchasing goods, paying utility bills, transferring money, booking flight etc. with a financial instrument (such as a credit card or a digital currency) using smart phones or computers. A plethora of these e-wallets are provided online for downloading through “apps” to support both point of sale transactions and peer-to-peer transactions between individuals. Being preloaded with currency by the user, they are designed to be convenient to them over the traditional-wallets, by providing better manageability over their payments, accounts, receiving of offers, alerts from merchants, storing digital receipts and warranty information and being secure by requiring to access only through correct passphrase, password and such authentication information.

A number of IT companies, Banks, Telecoms firms, online e-commerce portal, taxi-services, supermarket chains etc. provide e-wallets. A number of personally identifiable information (PII's) of the customer like his name, mobile phone number and his protected personal information like Customer card numbers, secret PIN, net banking credentials etc is permanently stored in e-wallets, requiring just final authorization from the user through means like biometrics authentication, one-time passwords(OTP) etc. The payment process involves security mechanisms like certificate pinning and use of encryption.



Threats to E-Wallets and countermeasures

Impersonation, SIM swapping

Impersonation occurs when a fraudster steals information and then poses as a genuine user to do a transaction using the stolen e-wallet details and password.

SIM swaps occurs when fraudsters first collect the user's information, and use it to get his mobile phone SIM card blocked, and obtain a duplicate one by visiting the mobile operator's retail outlet with fake identity proof. The mobile operator deactivates the genuine SIM card,

which was blocked, and issues a new SIM to the fraudster who then generates one-time passwords using stolen information.



For prevention against Impersonation and SIM swapping attacks:

- Avoid falling prey to social engineering tricks: Financial service provid-

ers and support staff will never ask their customers for sharing their private information such as passwords or payment account numbers over email requests or phone inquiries etc.

- Some Mobile network operators send an SMS to alert their customers of a SIM swap, the affected customer can act and stop this fraud in its tracks by contacting the mobile operator immediately.

Man-in-the-middle attack and Phishing

Sophisticated threats like Man-in-the-Browser or Man-in-the-Middle attacks intercept online transactions by reading payment data from the Internet browser while the user is typing his credit card or bank account details. Phishing attacks are used to steal users' login details and personal data, making e-wallet accounts susceptible to fraud.



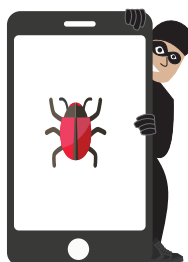
For prevention against phishing attacks:

- The URL of the web-page should be verified, by establishing the authenticity of the website by validating its digital certificate.

- To do so, go to File > Properties > Certificates or double click on the Pad-lock symbol at the upper right or bottom corner of the browser window. 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.

Malware Attacks

Malware attacks on apps have threatened the safety of user's money. An attacker can inject a malware to attack the app and collect details from his phone to misuse it.



For prevention against Malware attacks:

- Keep the wallet software up to date: Using the latest version of software allows receiving important stability and security fixes timely. Updates can prevent problems of various severities, include new useful features and help keep the wallet safe. Installing updates for all other software on

the computer or mobile is also significant to keep the wallet environment safer.

- 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.





Best practices for users to remain safe while using e-wallets

- **Enable Passwords On Devices:**

Strong passwords should be enabled on the user's phones, tablets, and other devices before e-wallets can be used. Additional layers of security provided by these devices should be used.

- **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.

- **Install Apps From Trusted Sources:**

Reading the user ratings and reviews can provide some clues about the integrity of the e-wallet app. The user must check for the e-wallet provider to be showing strong legacy of securely, reliably and conveniently handling sensitive financial data and providing customer support (in the event of card loss or account fraud).

- **Keep Login Credential Secure:**

Avoid writing down information used to access the digital wallets in plain view or storing them in an unprotected file to avoid their misuse.

- **Create a Unique Password for Digital Wallet:**

Use hard-to-guess password unique to the digital wallet to prevent against the risk of unauthorized access.

- **Stay vigilant and aware of cellphone's network connectivity status and register for Alerts through SMS and emails:**

The user should not switch off his cellphone in the event when numerous annoying calls are received, rather answering the calls should be avoided. This could be a ploy to get him to turn off his phone or put it on silent to prevent him from noticing that his connectivity has been tampered with. The customer should realize that when he is not receiving any calls or SMS notifications for a long time against his e-wallet uses, he should make enquiries with his mobile operator to be sure about not falling victim to such scam.

- **Identify Points of Contact in case of Fraudulent Issues:**

For any fraudulent activity occurring on the user's account in the scenarios like when phone is lost or stolen, an individual card stored in the wallet is lost or account has been hacked, appropriate points of contact for resolving the issues should be understood by the user. The user must completely understand the e-wallet providers contract terms and conditions.



SAFETY MEASURES TO PROTECT YOUR MOBILE PHONE



Enable Autolock and a Strong Passcode. Consider changing it frequently



Record your phone's unique ID number (IMEI number)



Make sure you log off from banking and other important Apps in your mobile phone after use



Consider tracking software



Regularly back up your Mobile phone

WHAT TO DO IF YOUR MOBILE PHONE IS LOST



Report theft of your mobile phone to your bank and nearest police station immediately



Try to locate your phone via GPS



Block your SIM card and Apply for a duplicate SIM card



Don't forget to remotely lock your phone



Change your important passwords immediately



Best practices to avoid Financial Frauds

Avoid using open Wi-Fi for making payments



Never handover your device to strangers

Keep a watch on transaction logs and alerts



Disclose your banking details only in secure payment websites

Immediately block your SIM if your device gets lost or stolen



Always verify and install authentic e-wallet Apps

Ensure that you securely dispose your payment receipts & bank statements



Report promptly the theft or loss of your card on the toll free numbers

Refrain from clicking suspicious links received in SMS or email



Use strong passwords and change frequently



POINT OF SALE

The point of sale (POS) is the place where a retail transaction occurs and the merchant calculates the amount owed by the customer, indicates the amount, prepares an invoice for the customer, and indicates the options for the customer to make payment. It is also the point at which a customer makes a payment to the merchant in exchange for goods or after provision of a service. After receiving the payment, the merchant issues a receipt for the transaction, this is usually printed, but is increasingly being dispensed with by sending it electronically.



POS systems consist of hardware as well as software that tell the hardware what to do with the information it captures. When consumers use a credit or debit card at a POS system, the information stored on the magnetic stripe of the

card is collected and processed by the

attached device. The data stored on the magnetic stripe is referred to as Track 1 and Track 2 data. Track 1 data is information associated with the actu-

al account and it includes items such as the cardholder's name as well as the account number. Track 2 data contains information such as the credit card number and expiration date.

Threats to POS Systems:

Skimming

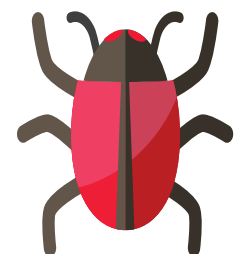
Skimming is an electronic method of capturing a victim's personal information used by identity thieves. The skimmer is a



small device that scans a credit/debit card and stores the information contained in the magnetic strip. Skimming can take place during a legitimate transaction at a business.

POS Malware

Point-of-sale malware (POS malware) is a type of malicious software (malware) that is used by cybercriminals to target



point of sale (POS) terminals with the intent of obtaining credit card and debit card information by reading the device memory from the retail checkout point of sale system.

Best Practices for Users to remain safe

Owners and operators of POS systems should follow best practices to increase the security of POS systems and prevent unauthorized access.

For organizations / service providers:

- **Update POS Software Applications:**
Keep all POS Systems regularly updated including POS application software.
- **Use Antivirus:**
It is suggested to continually update the antivirus programs for it to be effective on a POS network.
- **Install a Firewall:**
Firewalls should be utilized to protect POS systems from outside attacks. A firewall can

prevent unauthorized access to, or from, a private network by screening out traffic from hackers, viruses, worms, or other types of malware specifically designed to compromise a POS system.

- **Restrict Access to Internet:**
Apply access control lists on the router configuration to limit unauthorized traffic to POS devices.
- **Disallow Remote Access:**
Cyber Criminals can exploit remote access configurations on POS systems

to gain access to these networks. To prevent unauthorized access of POS systems, disallow remote access to the POS network at all times.

- **Review all Logs:**
Organizations and merchants providing POS services should review all system logs for any strange or unexplained activity on a regular basis.
- Encrypt transmission of card holder data across open, public network.

For Merchants:

- **Update POS Software Applications:**
Keep all POS Systems regularly updated including POS application software.
- **Review all Logs:**
Organizations and merchants providing POS services should review all system logs for any strange or unexplained activity on a regular basis.
- **Account Lock out policy:**
Locking out accounts after N number of incorrect login attempts.

- POS systems should not be used for general internet access by retailers.
- **Use Strong Passwords:**
All POS devices owners should change passwords to their POS systems on a regular basis, using unique account names and complex passwords.
- Merchants should ensure that all their Wi-Fi and internet connections are secured. Merchants may use a network name that is extremely generic but unique keeping the network simple and inconspicuous. In addition,

Merchants may modulate the signal strength of their Wi-Fi network so that it does not extend too far from the area of use or shop or building.

- Ensure that no electronic / magnetic devices are attached with POS systems. Enter the PIN numbers in a secret manner.
- Merchants should always purchase POS Systems from reputable dealers.
- If any suspected transactions are observed, contact the service provider / bank immediately.





MICRO ATMS

Micro ATMs are Point of Sale(PoS) Devices that work with minimal power, connect to central banking servers through GPRS, thereby reducing the operational costs considerably. Micro ATM solution enables the unbanked rural people to easily access micro banking services in a very effective manner.

How to Use Micro ATMs

The basic interoperable transaction types that the micro ATM will support are:

1. Deposit
2. Withdrawal
3. Funds transfer
4. Balance enquiry and mini-statement.

The micro ATM will support the following means of authentication for interoperable transactions:

1. Aadhaar + Biometric
2. Aadhaar + OTP
3. Magnetic stripe card + Biometric
4. Magnetic stripe card + OTP
5. Magnetic stripe card + Bank PIN

Threats to Micro ATMs:

Data Vulnerabilities

With respect to POS data vulnerabilities, there are three specific areas that should be given attention including data in memory; data in transit; data at rest. Data in memory in this context is when the card track data is brought into the system at the POS system via a POI (Point of Interface or some other input device). Data in memory is nearly impossible to defend if an attacker has access to the POS system. Traditionally, data input into the POS system was in memory in clear text, which is what allowed, attackers; memory scrapers to be very

successful. The way to minimize this risk is by encrypting the card data as soon as possible and keeping it encrypted to the maximum extend throughout its life within the system. Point to Point Encryption (P2PE) could be used to address the issue of encrypting data in memory.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can obtain victim's credit card number using a small electronic device near the card acceptance slot and store hundreds of victim's credit card numbers.

Social Engineering

Social engineering involves gaining trust - hence the fraudster poses as a member of staff. 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 micro ATM machine and requires assistance.

Best Practices for Users to remain safe

- | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Before using micro ATM, please ensure that there are no strange objects in the insertion panel of the ATM(to avoid skimming) • Cover the PIN pas while entering PIN. Destroy the transaction receipts securely after reviewing. • Change ATM PIN on a regular basis. • Keep a close eye on bank statements, and dispute any unauthorized charges or withdrawals immediately. | <ul style="list-style-type: none"> • Shred anything that contains credit card number written on it.(bills etc) • Notify credit/debit card issuers in advance for change of address. • Don not accept the card received directly from bank in case if it is damaged or seal is open. • Do not write PIN number on credit/debit card. • Do not disclose Credit Card Number/ATM PIN to anyone. • Do not hand over the card | <p>to anyone, even if he/she claims to represent the bank.</p> <ul style="list-style-type: none"> • Do not get carried away by strangers who try to help you use the micro-ATM machine. • Do not transfers or share account details with unknown/non validated source. • In case of any suspected transactions or loss of cards, contact the service provider/bank immediately. |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Enable your mobile phone number and e-mail with your banking transactions for timely alerts

Never respond to phone calls / SMS / e-mail asking to update or verify your banking details like PIN, CVV, Credit / Debit card details etc.,



Check your bank accounts regularly to make sure there are no unusual or unauthorized transactions

Before using ATM please ensure that there are no strange objects like skimmers fixed to the machine



ONLINE BANKING

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 threat and risks.

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.



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 ver-

sions/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 ANY-

ONE 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 mim-

ic 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, dis-

played 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





SECURITY TIPS FOR SAFE ONLINE SHOPPING

सी डैक
CDAC



Keep computer OS updated

Make sure your PC is secured with an antivirus, anti spyware, firewall, system updated with all patches

Check the security aspects of the website

Check whether the site is secured with https or padlock on the browser address bar

Avoid saving card details in shopping websites

Track your card statements frequently for any unknown transactions and immediately after making any payment

Don't save your payment details

After finishing your online shopping clear all the web browser cookies and turn off your PC

Use Secured Networks

Always use secured Internet connection. Avoid using public Wi-Fi networks

Don't click on links offering discounts/ prizes

It is always better to check in the original website for offers rather than clicking on links

Beware of phishing emails

Remember legitimate business people never send emails like "confirm your payment, purchase and account detail"

Change passwords frequently

Don't use a single password for a long time, change your email id, bank account, credit-debit card passwords frequently

Different passwords for different websites

If one of your password is cracked all other accounts with same password may be compromised. So use different passwords

For more details / queries on Cyber Security visit or call us to our Toll free number



The increasing usage of Smartphone's 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.



MOBILE BANKING

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 prevent 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/Smishing/Vishing Attack

An attacker attempts phishing on to a mobile phone through SMS (Short Message Service), text message, telephone call, fax, voice-mail 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

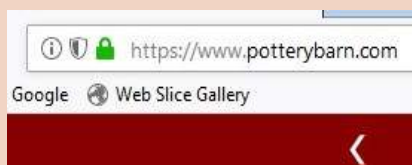
Market. User can alternatively check the Bank's website for the details of the ways to receive App download URL, whether in the response to his SMS or email to the bank and then install the application. The app from any other third party source should not be downloaded.

Best practices for users to be safe while doing Online shopping

Before you log on and make your first purchase, keep these ideas in mind to protect your credit card and keep your bank account information safe:

- **Only visit secure shopping websites—look for the "lock."** Check the address bar for a padlock symbol indicating

it's a secure website. Also, addresses beginning with "https" (and not just "http") indicate additional web security.



- **Shop online only with a secure network.** Although you might be enjoying a nice cup of coffee at a coffee shop, avoid using the public Wi-Fi in order to keep your payment information safe.
- **Protect your personal information.** Never click the



box to “remember” or save your password or credit card information. It only



takes a few seconds to enter this information when you revisit a site. (This is not only a good idea for shopping, but should be a general rule for keeping your passwords safe.)

- **Watch out for frauds.** With online shopping, you typically receive a confirmation for the order and another when shipping occurs. One current phishing scam sends a fake email indicating a problem with your order and includes a link or attachment to click. Another phishing scam is targeting Amazon shoppers. Amazon will never send you an unsolicited email asking for sensitive personal information like your social security num-

ber, tax ID, bank account number, credit card information, ID questions like “mother’s maiden name” or account password. If



you receive a suspicious email, please report it immediately by sending it as an attachment to stop-spoofing@amazon.com. (Likewise, if you are reporting a suspicious URL, put it in the body of the email and send it to stop-spoofing@amazon.com.)

- **Monitor your purchases.** This is another list to “check twice.” Hopefully, you are reviewing your credit card and bank statements throughout the year. During the holidays, it is even more important to be vigilant so you can catch any suspicious activity on your accounts.
- **Avoid use of cookies:** Cookies are typically

stored on your computer’s Internet browser by default. The purpose of cookies is to store settings and information for web pages that you have accessed. Turn off cookies from settings of the web browser and apps that you use for shopping.



- **Use Secure payment methods:** Only shop on sites that take secure payment methods, such as credit cards, as they likely give you buyer protection just in case there’s a dispute.



Watch out for fake shopping Apps

- Thieves are trying to steal your credit card and identity with fake shopping apps. Be sure you are downloading the legitimate app by getting it from the company’s official website or, if downloading from an app store directly, check to see it’s been around for a few years and has high ratings from many users. Never be the first to download a new shopping app.
- If you are interacting with brands on social media, make sure they are “verified,” with the little blue checkmark by their profile, which means the company is legit.



MOBILE APPLICATION SECURITY

सी डैक
CDAC

Use only
official stores for
downloading Apps



Do good research
about apps
and their developers
by reading the reviews

Reset your phone
to factory settings to
remove any malware



Check for spelling
mistakes in the title
or description

Make sure you
review and manage
permissions for each
app you download



Beware of apps
that promise
shopping discounts

Uninstall apps when
you no longer use



Avoid installing apps
by clicking
on links in emails,
social media etc.,

Always keep an
updated
anti virus security
solution installed



Look at the publish
date. A fake app
will have a recent
publish date



For more details / queries on Cyber Security visit or call us to our Toll free number



Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

www.
InfoSec
awareness.in

1800 425 6235

For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents
<http://cert-in.org.in/>

www.
cyberswachhtakendra.
gov.in



CYBER LAWS IN INDIA



When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all-pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities

in cyberspace. Hence the need for Cyberlaws in India. Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. In May 2000,

both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.



39



LAW

LAW

LAW

LAW

LAW



- **Email Account Hacking**

If victim's email account is hacked and obscene emails are sent to people in victim's address book. Provisions Applicable:- Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.

- **CreditCardFraud**

Unsuspecting victims would use infected computers to make online transactions. Provisions Applicable:- Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

- **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs**

All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information. Provisions Applicable:- Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

- **Phishing and Email Scams**

Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information) Provisions Applicable:- Section 66, 66A and 66D of IT Act and Section 420 of IPC

- **Theft of Confidential Information**

Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees. Provisions Applicable:- Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.

- **Tax Evasion and Money Laundering**

Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities. Provisions Applicable: Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.

- **Online Share Trading Fraud**

It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds. Provisions Applicable: Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC

Indian Penal Code (IPC)

The Indian Penal Code (IPC) is the criminal code of India. It is a comprehensive code intended to cover all substantive aspects of criminal law. The code was drafted in 1860 on the recommendations of first law commission of India established in 1834 under the Charter Act of 1833 under the Chairmanship of Lord Thomas Babington Macaulay. It came into force in British India during the early British Raj period in 1862. However, it did not apply automatically in the Princely states, which had their own courts and legal systems until the 1940s. The Code has since been amended several times and is now supplemented by other criminal provisions.



The Indian Penal Code works on the basic format and it lists all the cases and punishments that are liable to be charged on a person committing a crime. It covers any and every person of Indian Origin. The Indian Penal Code of 1860 is subdivided into twenty-three chapters comprising of five hundred and eleven sections. Although every Indian individual comprises under Indian Penal Code, the military, air and other armed forces are exceptions to IPC and contain their own tribunals for the punishment against a crime or an offence.

Importance of IPC

The Indian Penal Code holds a very important place when it comes to setting the rules and regulations and thus proves to be of a great importance for the system to be operated in an appropriate way. IPC is considered as one of the main criminal codes of India.

IPC and Banking Frauds Perpetrators of frauds in banking transactions are liable to be prosecuted under the criminal law of the country for which adequate provisions of punishment have been prescribed under the Indian Penal Code, 1860. Some of the important provisions of the IPC in this regard are discussed hereunder-





- **Section 403 in Indian Penal Code**-Dishonest misappropriation of property: According to this provision, whoever dishonestly misappropriates or convert to his own use, any movable property, shall be punished with imprisonment for a term which may extend to two years or with fine or with both.
- **Section 405 in Indian Penal Code** -Criminal breach of trust: According to this provision, anybody entrusted with the property dishonestly misappropriates or converts to his own use or dishonestly uses or disposes of that property in violation of any 3 direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, which he has made touching the discharging of such trust, commits criminal breach of trust.
- **Section 406 in Indian Penal Code** prescribes punishment for criminal breach of trust which is imprisonment extending to three years or fine or both.
- **Section 409 in Indian Penal Code** prescribes higher imprisonment of upto ten years in respect of criminal breach of trust by a public servant or by a banker or merchant or agent.
- **Section 463 in Indian Penal Code** -Forgery: It is defined as- “ Whoever makes any false document or false electronic record or, part of a document, or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery”.
- **Section 465 in Indian Penal Code** prescribes a punishment for forgery which is imprisonment for a term which may extend to two years or with fine or with both.
- **Section 489-A in Indian Penal Code** – Counterfeiting of currency notes: This section provides that whoever counterfeits, or knowingly performs any part of the process of counterfeiting, any currency note or bank note, shall be punished for imprisonment for life, or with imprisonment of eight years
- Cheating is described under Section 415 and Implications of fraud are found u/s **sections 421,422,423 and 424 of IPC.**
- The legal definition of Fraud is “A false representation of a matter of fact whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed that deceives and is intended to deceive another so that the individual will act upon it to her or his legal injury.



- **Section 415 in The Indian Penal Code 415. Cheating.** — Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to “cheat”.
Explanation. — A dishonest concealment of facts is a deception within the meaning of this section.
- **Section 25 in The Indian Penal Code**
“Fraudulently”.—A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise. Implications of fraud are found in these following sections of IPC namely, 421,422,423 and 424.
- **Section 421 in Indian Penal Code:** Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors.
Whoever dishonestly or fraudulently removes, conceals or delivers to any person, or transfer or causes to be transferred to any person, without adequate consideration, any property, intending thereby to prevent, or knowing it to be likely that he will thereby prevent, the distribution of that property according to law among his creditors or the creditors of any other person, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both
- **Section 422 in Indian Penal Code:** Dishonestly or fraudulently preventing debt being available for creditors. Whoever dishonestly or fraudulently prevents any debt or demand due to himself or to any other person from being made available according to law for payment of his debts or the debts of such other person, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
- **Section 423 in Indian Penal Code:** Dishonest or fraudulent execution of the deed of transfer containing false statement of consideration.
Whoever dishonestly or fraudulently signs, executes or becomes a party to any deed or instrument which purports to transfer or subject to any charge any property, or any interest therein, and which contains any false statement relating to the consideration for such transfer or charge, or relating to the person or persons for whose use or benefit it is really intended to operate, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
- **Section 424 in Indian Penal Code:** Dishonest or fraudulent removal or concealment of property. Whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.



Frauds relating to computers

To provide efficient and fast service, most of the branches of the banks except the ones in the rural and remote areas have been computerized. Not many frauds relating to computers have yet been reported so far as computerization in the Indian banks is of recent origin. But in the western countries where virtually everything is computerized, a large number of cyber crimes in the banking sector are reported on a regular basis.

There is a need to analyse the nature of such crimes so that appropriate preventive measures may be devised. Normally following types of frauds are committed-

- Spy software are devised by the cyber criminals to crack the passwords. They enter into the computer system of the banks and manipulate the data to transfer the money from other's accounts.
- Computer virus are created by the mischief mongers which find way into the computer system by way of e-mails. These virus destroy the data

stored in the computers and slow down the entire computer system. It is sometimes alleged that the manufacturers of anti-virus software themselves create virus so that their product may be sold in the market.

- Hackers are computer experts who steal the passwords and access the classified information stored in the computer system. They do not even fear to "raid" the government departments including military establishments to carryout their nefarious design to destroy and mutilate the data stored in the computer systems. Such acts

are committed normally not for any material gain but to derive mental satisfaction out of other's sufferings.

- Wire tapping is a crime committed by tapping the wire of the ATMs of the banks to withdraw money out of other person's account. The fraudster, in this case, attaches a wireless microphone to the telephone line connecting the ATM with the bank's computer and records signals through wire tapping while a customer is using the ATM. These signals are later on utilized for withdrawing money.

The Government of India enacted the Information Technology Act, 2000 to provide for punishment and penalties in respect of frauds committed in respect of computers. Section 43 of the said Act provides for hefty damages upto rupees ten lakhs payable by the offender to the person affected in case there are unauthorized acts committed in respect of another person's computer system like access, downloads or taking copies of the information or data stored, introduction of computer contaminant or computer virus, damages to the computer or its system etc. Further, the said Act also provides for punishment with imprisonment upto three years for tampering with computer source documents and for hacking the computer systems.

Information Technology Act, 2000(Amendment 2008) ,66C:

Fraudulently or dishonestly usage of identity.

An offender who fraudulently or dishonestly uses the photograph and other personal details of the victim for creating the fake profile is guilty of “identity theft”.

Punishment: which is punishable with “imprisonment up to three years and fine up to one lakh rupees”.

Section 469 in The Indian Penal Code:

If the fake profile contains objectionable content, it amounts to forgery for the purpose of harming reputation.

Punishment: which is punishable with “imprisonment up to three years and fine”.

Section 66 of the Information Technology Act, 2000:

If the offender dishonestly or fraudulently uses the fake profile to introduce viruses or other computer contaminants in computers or computer networks, or for spamming or for committing data theft.

Punishment: which is punishable with a “imprisonment up to three years or/and fine up to five lakh rupees”.

Section 43 in The Indian Penal Code

The word “illegal” is applicable to everything which is an offence or which is prohibited by law, or which furnishes ground for a civil action; and a person is said to be “legally bound to do” whatever it is illegal in him to omit.

Section 67 of the Information Technology Act:

If the offender posts obscene material on the fake profile.

Punishment: punishable with “imprisonment up to three years and with fine up to five lakh rupees”.

In the event of second or subsequent conviction with “imprisonment up to five years and with fine which may extend to ten lakh rupees”. Sections 292, 293 of the IPC may also be invoked against such offenders.

Section 67A of the Information Technology Act, 2000:

Publishing or transmitting of material containing the sexual explicit act, etc. in the electronic form

Punishment: If the fake profile contains “sexually explicit act or conduct”, the offender will invite more stringent punishment of “imprisonment up to five years and fine up to ten lakh rupees

The event of second or subsequent conviction, imprisonment up to seven years and fine up to ten lakh rupees”.

Section 67B of the Information Technology Act, 2000:

Publishing or transmitting of material depicting children in the sexual explicit act, etc. in the electronic form.

Punishment: If such sexually explicit act or conduct relates to children below 18 years of age, then even the people visiting that profile or promoting or advertising it (by posting links on their own profile) would invite the same punishment.

Section 471 in Indian Penal Code:

Whoever fraudulently or dishonestly uses as genuine any document which he knows or has reason to believe to be a forged document.

Punishment: The offence under section 471 is cognizable, non-bailable and non-compoundable, and is triable by magistrate of the first class

Section 420 in The Indian Penal Code:

Cheating and dishonestly inducing delivery of property

Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.



The various sections and corresponding punishments are as follows :

Section	Contents	Imprisonment	Fine
66	Hacking with computer system dishonestly or fraudulently	3 years or/and	500,000
66C	Identity Theft - fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person	3 years and	100,000
67	Publish or transmit Obscene material - 1st time Subsequent Obscene in elec. Form	3 years and 5 years and	500,000 10,00,000
67A	Publishing or transmitting material containing Sexually Explicit Act - 1sttime Subsequent	5 years and 7 years and	10,00,000 10,00,000
67B	Publishing or transmitting material containing Children in Sexually Explicit Act - 1st time Subsequent	5 years and 7 years and	10,00,000 10,00,000
67C	Contravention of Retention or preservation of information by intermediaries	3 years and	Not Defined

GUIDELINES TO REPORT FINANCIAL FRAUDS IN INDIA

Follow these steps if you find an unauthorized transaction on your account.

- Contact Your Bank. As per RBI regulations Illegal transaction if reported immediately bank will pay back the lost amount if bank finds there is no fault with the account holder.
- File a Fraud or Police Report.
- Block your current account and move your money to Your New Account or Card.
- Monitor Your Account and Credit Closely.



How to file a cyber crime complaint in India

According to the IT Act, a cyber crime comes under the purview of global jurisdiction. This means that a cyber crime complaint can be registered with any of the cyber cells in India, irrespective of the place where it was originally committed. At present, most cities in India have a dedicated cyber crime cell. List of all cyber crimes cells are given below.

Step 1:

The very first step to file a cyber crime complaint is to register a written complaint with the cyber crime cell of the city are currently in.

Step 2:

When filing the cyber crime complaint, you need to provide your name, contact details, and address for mailing. You need to address the written complaint to the Head of the Cyber Crime Cell of the city where you are filing the cyber crime complaint.

Step 3:

In case you are a victim of online harassment, a legal counsel can be approached to assist you with reporting it to the police station. Additionally, you may be asked to provide certain documents with the complaint. This would, however, depend on the nature of the crime.

Step 4:

Register a Cyber Crime FIR: If you do not have access to any of the cyber cells in India, you can file a First Information Report (FIR) at the local

police station. In case your complaint is not accepted there, you can approach the Commissioner or the city's Judicial Magistrate.

Step 5:

Certain cyber crime offenses come under the Indian Penal Code. You can register a cyber crime FIR at the nearest local police station to report them.

Step 6:

You can report at CERT In official website.

CERTIn is the national nodal agency for responding to computer security incidents as and when they occur. As per the Information Technology Amendment Act 2008 and Section 70B of IT Act 2000, CERTIn has been designated to serve as the national agency to perform the following functions in the area of cyber security: Collection, analysis and dissemination of information on cyber incidents, Forecast and alerts of cyber security incidents, Emergency measures for handling cyber security incidents, Coordination of cyber incident response activities. Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents. Such other functions relating to cyber security as may be prescribed.





CYBERCRIME POLICE STATIONS

Place	Address
Assam	CID HQ,Dy.SP. Assam Police Ph: +91-361-252-618, +91-9435045242 E-mail: ssp_cod@assampolice.com
Bangalore	Cyber Crime Police Station C.O.D Headquarters, Carlton House, # 1, Palace Road, Bangalore – 560 001 +91-80-2220 1026 +91-80-2294 3050 +91-80-2238 7611 (FAX)
Delhi	CBI Cyber Crime Cell: Superintendent of Police, Cyber Crime Investigation Cell Central Bureau of Investigation, 5th Floor, Block No.3, CGO Complex, Lodhi Road, New Delhi – 3 +91-11-4362203, +91-11-4392424, E-Mail: cbiccic@bol.net.in
Pune	Deputy Commissioner of Police(Crime) Office of the Commissioner Office, 2, Sadhu Vaswani Road, Camp,Pune 411001 +91-20-26123346, +91-20-26127277, +91-20-2616 5396 +91-20-2612 8105 (Fax) E-Mail: crimecomp.pune@nic.in, punepolice@vsnl.com
Jharkhand	IG-CID,Organized Crime Rajarani Building,Doranda Ranchi, 834002 Ph: +91-651-2400 737/ 738 E-mail: a.gupta@jharkhandpolice.gov.in
Haryana	Cyber Crime and Technical Investigation Cell, Joint Commissioner of Police Old S.P.Office complex, Civil Lines, Gurgaon E-mail: jtcp.ggn@hry.nic.in
Jammu	SSP,Crime, CPO Complex,Panjtirthi, Jammu-180004 Ph: +91-191-257-8901 E-mail: sspcrmjmu-jk@nic.in
Meghalaya	SCRB,Superintendent of Police, Meghalaya Ph: +91 98630 64997 E-mail: scrb-meg@nic.in
Bihar	Cyber Crime Investigation Unit Dy.S.P.Kotwali Police Station, Patna Ph: +91 94318 18398, E-mail: cciu-bih@nic.in
Chennai	Assistant Commissioner of Police Cyber Crime Cell, Central Crime Branch, Commissioner office Campus Vepery, Chennai- 600007 Contact Details: +91-40-2345 2348, 2345 2350
For Rest of Tamil Nadu,	Cyber Crime Cell, CB, CID, Chennai Ph:+91 44 2250 2512 E-mail id: cbcyber@tn.nic.in

CYBERCRIME POLICE STATIONS

Place	Address
Hyderabad	Cyber Crime Police Station Crime Investigation Department, 3rd Floor, D.G.P. office, Lakdikapool, Hyderabad – 500004 +91-40-2324 0663, +91-40-2785 2274 +91-40-2785 2040, +91-40-2329 7474 (Fax)
Thane	3rd Floor, Police Commissioner Office Near Court Naka, Thane West, Thane 400601. +91-22-25424444, E-Mail: police@thanepolice.org
Gujarat	DIG, CID, Crime and Railways Fifth Floor, Police Bhavan Sector 18, Gandhinagar 382 018 +91-79-2325 4384, +91-79-2325 0798, +91-79-2325 3917 (Fax)
Madhya Pradesh	IGP, Cyber Cell, Police Radio Headquarters Campus, Bhadadhadaa Road, Bhopal (M.P.) Ph: 0755-2770248, 2779510
Mumbai	Cyber Crime Investigation Cell Office of Commissioner of Police office, Annex -3 Building, 1st floor, Near Crawford Market, Mumbai-01. +91-22-22630829, +91-22-22641261 E-mail id: officer@cybercellmumbai.com
Himachal Pradesh	CID Cyber Cell , Superintendent of Police, Cyber Crime, State CID, Himachal Pradesh, Shimla-2 Ph: 0177-2621714 Ext: 191, 0177-2627955 E-mail:cybercrrcell-hp@nic.in,
Kerala	Hi-tech Cell, Police Head Quarters Thiruvananthapuram +91-471 272 1547, +91-471 272 2768, E-mail: hitechcell@keralapolice.gov.in
Orissa	Cyber Crime Police Station, CID, CB, Odisha, Cuttack-753001 Ph. No.0671-2305485, E-mail ID:- sp1cidcb.orphol@nic.in
Punjab	Cyber Crime Police Station DSP Cyber Crime, S.A.S Nagar,Patiala, Punjab, Ph: +91 172 2748 100
Uttar Pradesh	Cyber Crime Cell,, Agra Range 7,Kutchery Road, Baluganj,Agra-232001, Uttar Pradesh Ph:+91-562-2210551 e-mail: digraga@up.nic.in, cybercrimeag-up@nic.in, Cyber Crime Cell, Crime Branch, Law Enforcement Agency, Police Line, Agra – 282001



CYBER CRIMES MAPPING

WITH ITAA 2008, IPC AND SPECIAL AND LOCAL LAWS

Sl.No	Nature of complaint	Applicable section (s) and punishments under ITA 2000 & ITAA 2008	Applicable section (S) under other laws and punishments
1	Mobile phone lost/stolen	-	Section 379 IPC 3 years imprisonment or fine or both
2	Receiving stolen computer/mobile phone / data (data or computer or mobile phone owned by you is found in the hands of someone else.)	Section 66 B of ITAA 2008-3 year imprisonment or fine up to rupees one lakh fine or both	Section 411 IPC - 3 years imprisonment or fine or both
3	Data owned by you or your company in any form is stolen	Section 66c of ITAA 2008- 3 years imprisonment or fine up to rupees five lakh or both	Section 379 IPC - 3 years imprisonment or fine or both
4	A Password is stolen and used by someone else for fraudulent purpose	Section 66c of ITAA 2008- 3 years imprisonment or fine up to rupees one lakh Section 66D ITAA 2008 - 3 years imprisonment and fine up to Rupees one Lakh	Section 419 IPC - 3 years imprisonment or fine Section 420 IPC - 7 years imprisonment and fine
5	An e-mail is read by someone else by fraudulently making use of password	Section 66 of ITAA 2008- 3 years imprisonment or fine up to Rupees five lakh or both Section 66C of ITAA 2008 - 3 years imprisonment and fine up to Rupees one lakh	
6	A Biometric thumb impression in misused	Section 66C of ITAA 2008- 3 years imprisonment and fine up to Rupees one lakh	
7	An electronic signature or digital signature is misused	Section 66C ITAA 2008 - 3 years imprisonment and fine up to Rupees one lakh	
8	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66D of ITAA 2008 - 3years imprisonment and fine up to Rupees one lakh	Section 419 IPC - 3 years imprisonment or fine or both
9	Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge	Section 66E of ITAA 2008 - 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC - Two years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction
10	Tampering with computer source Documents	Section 65 of ITAA 2008- 3 years imprisonment or fine up to Rupees two lakh or both Section 66 of ITAA 2008 - 3 years imprisonment or fine up to Rupees five lakh or both	

CYBER CRIMES MAPPING

WITH ITAA 2008, IPC AND SPECIAL AND LOCAL LAWS

Sl.No	Nature of complaint	Applicable section (s) and punishments under ITA 2000 & ITAA 2008	Applicable section (S) under other laws and punishments
11	Data Modification	Section 66 of ITAA 2008 - 3 years imprisonment or fine up to Rupees five lakh or both	
12	Sending offensive messages through communication service, etc.		Section 500 IPC - 2years or fine or both s Section 504 IPC - 2years or fine or both section 506 IPC - 2 years or fine or both - if threat be to cause death or grievous hurt, etc. - 7 years or fine or both Section 507 IPC - 2 years along with punishment under section 506 IPC Section 508 IPC - 1 year or fine or both Section 509 IPC - 1 years or fine or both of IPC as applicable
13	Publishing or transmitting obscene material in electronic form	Section 67 of ITAA 2008 first conviction - three years and 5 lakh second or subsequent conviction - 5 years and up to 10 lakh	Section 292 IPC - two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent.
14	Publishing or transmitting obscene material in electronic form	Section 67A of ITAA 2008 first conviction - three years and 5 lakh second or subsequent conviction - 5 years and up to 10 lakh	Section 292 IPC - two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent.
15	Publishing or transmitting obscene material in electronic form	Section 67B of ITAA 2008 first conviction - three years and 5 lakh second or subsequent conviction - 5 years and up to 10 lakh	Section 292 IPC - two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent.
16	Misusing a Wi-Fi connection for acting against the state	Section 66 - three years imprisonment or fine up to Rupees five lakh or both section 66 F - life imprisonment of ITAA 2008	
17	Planting a computer virus that acts against the state	Section 66 - 3 years imprisonment or fine up to Rupees five lakh or both 66F - life imprisonment	
18	Conducting a denial of service attack against a government computer	Section 66 of ITAA 2008 - 3 years imprisonment or fine up to Rupees five lakh or both section 66F of ITAA 2008 - life imprisonment	



CYBER CRIMES MAPPING

WITH ITAA 2008, IPC AND SPECIAL AND LOCAL LAWS

Sl.No	Nature of complaint	Applicable section (s) and punishments under ITA 2000 & ITAA 2008	Applicable section (S) under other laws and punishments
19	Stealing data from a government computer that has significance from national security perspective	Section 66 of ITAA 2008 - 3 years imprisonment or fine up to Rupees five lakh or both 66F - life imprisonment.	
20	Not allowing the authorities to decrypt all communication that passes through your computer or network.	Section 69 of ITAA 2008 imprisonment up to 7 years and fine	
21	Intermediaries not providing access to information stored on their computer to the relevant authorities	Section 69 of ITAA 2008 imprisonment up to 7 years and fine	
22	Failure to Block Web Sites. When ordered	Section 69A of ITAA 2008 imprisonment up to 7 years and fine	
23	Sending threatening messages by E-Mail.		Section 504- 2 years or fine or both
24	Word, gesture or act intended to insult the modesty of a woman		Section 509 IPC – 1 year or fine or both – IPC as applicable
25	Sending defamatory messages by E-Mail		Section 500 IPC – 2 years or fine or both
26	Bogus Web sites, Cyber frauds	Section 66D of ITAA 2008 – 3years imprisonment and fine up to Rupees one lakh	Section 419 IPC – 3 years imprisonment or fine Section 420 IPC – 7 years imprisonment and fine
27	E-Mail Spoofing	Section 66C of ITAA 2008 – 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC – 2 years or fine or both Section 468 IPC – 7 years imprisonment and fine
28	Making a false document	Section 66D of ITAA 2008- 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC - 2 years or fine or both
29	Forgery for purpose of cheating	Section 66D of ITAA 2008 – 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC – 7 years imprisonment and fine
30	Forgery for purpose of harming reputation	Section 66D of ITAA 2008 – 3 years imprisonment and fine up to Rupees one lakh	Section 469 IPC – 3 years and fine

CYBER CRIMES MAPPING

WITH ITAA 2008, IPC AND SPECIAL AND LOCAL LAWS

Sl.No	Nature of complaint	Applicable section (s) and punishments under ITA 2000 & ITAA 2008	Applicable section (S) under other laws and punishments
31	E-Mail Abuse		Sec. 500 IPC – 2 years or fine or both
32	Punishment for criminal intimidation		Sec. 506 IPC – 2 years or fine or both – if threat be to cause death or grievous hurt, etc. – 7 years or fine or both
33	Criminal intimidation by an anonymous communication		Sec. 507 IPC – 2 years along with punishment under section 506 IPC
34	Copyright Infringement	Section 66 of ITAA 2008 – 3 years imprisonment or fine up to Rupees five lakh or both	Sec. 63, 63B Copyright act 1957
35	Theft of Computer Hardware		Sec. 376 IPC 3 years imprisonment or fine or both
36	Online Sale of Drugs		NDPS Act
37	Online Sale of Arms		Arms Act

References

- <https://www.bankbazaar.com/ifsc/digital-payment.html?ck=Y%2BziX71XnZjIM9ZwEflsyDYl-RL7gaN4W0xhuJSr9lq7aMYwRm2IPACTQB2XBBtGG&rc=>
- <http://digitalindia.gov.in/empowerment>
- http://serviceonline.gov.in/resources/homePage/99/PDF/pkg_dipankar.pdf
- <https://s3.amazonaws.com/DFIAA/Handbook%20Digital%20Finance%20for%20Rural%20India-%20FINAL%20Final%20%281%29.pdf>
- <https://www.mapsofindia.com/my-india/government/beware-over-30-lakh-debit-cards-are-at-risk>
- <https://pdfs.semanticscholar.org/bb7d/b61404fbccf2b6beb91577bb21c115b00edf.pdf>
- <https://upipayments.co.in/aadhaar-enabled-payment-system/>
- <http://www.cert-in.org.in/>
- <https://www.thehindubusinessline.com/info-tech/bhim-may-expose-you-to-data-theft/article9485614.ece>
- <https://ifflab.org/how-to-file-a-cyber-crime-complaint-in-india/>

To Share Tips / Latest News, mail us to

isea@cdac.in

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events all over India.

About C-DAC

Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Ministry of Electronics and Information Technology (MeitY) for carrying out R&D in IT, Electronics and associated areas.

C-DAC has today emerged as a premier R&D organization in IT&E (Information Technologies and Electronics) in the country working on strengthening national technological capabilities in the context of global developments in the field and responding to change in the market need in selected foundation areas. In that process, C-DAC represents a unique facet working in close junction with MeitY to realize nation's policy and pragmatic interventions and initiatives in Information Technology. As an institution for high-end Research and Development (R&D), C-DAC has been at the forefront of the Information Technology (IT) revolution, constantly building capacities in emerging/enabling technologies and innovating and leveraging its expertise, caliber, skill sets to develop and deploy IT products and solutions for different sectors of the economy, as per the mandate of its parent, the Ministry of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India and other stakeholders including funding agencies, collaborators, users and the market-place.

For queries on Information security

Call us on Toll Free No.

1800 425 6235

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

between 9.00 AM to 5.30 PM

Subscribe us on



<https://www.youtube.com/c/InformationSecurityEducationandAwareness>

Follow us on



<https://twitter.com/InfoSecAwa>

Connect us with



<https://www.facebook.com/infosecawareness>



Ministry of Electronics & Information Technology
Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार

A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Sitapal Highway,
Pahadi Sharaf Via Keshavnagar (Post), Hyderabad - 501510, Telangana (India)

Nalanda Building, No. 1 Shivabagh Sanyam Theatre Road,
Ameerpet, Hyderabad - 500016, Telangana (India)