SOUTH INDIAN Bank
Experience Next Generation Banking

STUDENTS' ECONOMIC FORUM

OPEN ACCESS www.sib.co.in

To kindle interest in economic affairs...
To empower the student community...

ho2099@sib.co.in

October 2015

Theme 287

INFORMATION SECURITY, ELECTRONIC BANKING, TECHNOLOGY RISK MANAGEMENT & CYBER FRAUDS - PART II

A monthly publication from South Indian Bank

24th Year of Publication

www.southindianbank.com

| Simple documentation procedures | No prepayment penalty | Repayment tenure up to 30 years*
| Low processing fee | No hidden charges | Flexible & fixed interest options

SOUTH INDIAN Bank

Experience Next Generation Banking

The South Indian Bank Ltd., Regd. Office, SIB House,P.B. No. 28, Thrissur, Kerala, PIN-680 001
Ph: 0487 2420020, Fax: 0487 2426187, Toll Free (India): 1800-843-1800, 1800-425-1809 (BSNL)
Email: sibcorporate@sib.co.in | CIN : L65191KL1929PLC001017

South Indian Bank is a member of BCSBI and is committed to treat customers in a fair, transparent and non-discriminatory manner.

http://www.facebook.com/thesouthindianbank

Theme No: 287: Information Security, Electronic Banking, Technology Risk Management & Cyber Frauds - Part II

A well informed customer will make the policy makers as well as organisations which produce goods and services more responsive to the customer needs. This will also result in healthy competition among organisations and improve the quality of goods and services produced. The "SIB Students' Economic Forum" is designed to kindle interest in economic affairs in the minds of our younger generation. This month we continue the discussion on Recommendation of the working group headed by Sri G Gopalakrishna on electronic banking /delivery channels.

What are the important security measures recommendated for ATMs?

1. There should be a unique ID for every ATM for easy identification.
2. Configuration and tuning of ATMs should be robust
3. ATM cameras should give clear picture of the person doing the transaction. ATM Centre should be properly lighted so that photo taken will be clear. Banks may install additional cameras also to capture the picture of the customer taking the money.
4. Antivirus and Firewall system
5. ATM locations may be provided with security persons
6. At a time only one person should be allowed to operate the ATM
7. ATM's key at the time of installation may be destroyed
8. There should be controls and check measures for generation, transmission and loading of ATM
9. IP Sec may be used for the transmission of messages between the ATM and switch

Briefly explain the switch security recommendations?

1. Card/account authentication and validation using switch
2. Hardware Security Module may use PIN based authentication
3. Daily limit for transaction concept to be introduced to reduce the risk of card misuse
4. First ATM transaction should have PIN verification

5. If the card holder enters wrong PIN, a certain number of times, then the card should be blocked
6. Firewall

The committee also suggested to have controls relating verification of card number

What are the suggestions for card based online transactions/ecommerce?

The committee suggested the following measures/ecommerce.

1. Second factor authentication should be introduced for e-commerce transactions
2. Email alerts to be sent on the registered Email id

Describe briefly regarding the recommendations of the committee on phone banking?

1. There should be suitable security measures for customer authentication through phone banking
2. Customer data like account number, status etc should not be stored in cache memory. After encryption the information provided by the customer on IVR to be send back to end host directly.
3. Only after the due verification change in critical details should be allowed and that too only through a branch.

What are the major mobile banking recommendations?

Major channels of mobile applications are the following

1. SMS (Short Messaging Services)
2. WAP (Wireless Access Protocol)
3. Web Browser Based
4. Mobile Application Client
5. Unstructured Supplementary Service Data (USSD)
6. IVR (Interactive Voice Response)

Important security measures recommended for the mobile banking are the following

1. Before allowing a transaction, authentication of the device with the service provider to be obtained which will ensure that no unauthorized devices are not connected to perform financial transactions.
2. Bank customer's password/User ID authentication
3. Two factor authentication through MPIN or higher standard and end-to-end encryption of MPIN is desirable
4. Storage of MPIN in a secured environment

What are the important debit card security measures suggested by the committee?

1. There should be a specific algorithm and verification at the switch level for the personalization of the card and generation of the card.
2. Delivery to be secured and only after the customer identification, delivery to be made
3. Activation of the card to be controlled
4. Cards to be blocked after the certain number of wrong attempts
5. SMS message to be sent to the customer's registered mobile number instantaneously on the usage of the card at any ATM, POS or E-commerce site.

Describe briefly recommendations of the committee regarding Anti-Skimming measures?

Illegal copying of the information from the magnetic strip of a credit or debit card is known as 'card skimming'. Once skimmers get the details of the card, then they will be able to create a fake or 'cloned card' with the details collected from the original card.

Following are the major suggestions regarding the anti-skimming

1. Creation of the awareness among the customers and branch personnels about the various methods of the skimming
2. ATM servicing may be done in the presence of bank officials and frequent or random inspection of off-site ATMs.
3. Security guards for all ATMs
4. Banks may request customers to provide / register their mobile numbers for alert purpose
5. Implementation of fraud monitoring software
6. Triggering of alerts for transactions which are not normal
7. Seperate pin for foreign users or separate activation for international usage

Some of the other suggestions are Jittering, chip based cards and pin based authorization

What are the security measures suggested by the working committee for internet banking?

1. Sensitive information should not be stored in HTML hidden fields, cookies or any other client-side storage. Critical web application should enforce SSL v3 or extended validation-SSL/TLS 1.0.128 bit encryption level for all online activities
2. In case of interruption, it should require normal user identification, authentication and authorization for re-establishment of session.

What are the authentication practices recommended for internet banking?

There are 3 basic factors for authentication.

1. Which the user knows (example: password, pin etc.)
2. Which the user has (example: ATM card, smart card etc.)
3. Which the user is (example: biometric characteristics, such as finger prints etc.) properly designed reliable multi factor authentication methods, capable of combating various cyber attack mechanism like Phishing, Key logging, Spyware/Malware and other internet based frauds, should be implemented.

Major two-factor techniques/methodologies for compacting cyber attacks include the following:

1. **Tokens**: - Tokens are physical devices and three types of tokens are a) USB token devices b) Smart Cards c) Password generating tokens

a. USB token devices:- It is plugged directly into computers USB port and hence it does not require installation of any special hardware on the user's computers. Once the USB token is recognized, in order to access the computer system, the customer has to enter his or her own password. It is difficult to duplicate USB tokens and they are tamper resistant. It is user friendly and easy to carry
b. Smart cards:-Smart cards contain microprocessor which enables it to store and process the data. It has the size of the credit card. If the reader attached to the customer computer recognizes the card then the customer is prompted to enter the password. Smart cards are easy to carry and easy to use, but it requires installation of hardware and software drivers on user's computers.
c. Password generating tokens: - Each time password generating token produces a code whenever it is used is known as one-time password (OTP). OTP is displayed on the screen of the token. The customer has to enter the name and regular passwords followed by the OTP into the bank's website and the customer will be authenticated if the both passwords are matched.

It is very difficult for cyber fraudsters to capture the detail. However it has got the logistics issues.

2. **SMS Based One Time Password**: - In this method the customer will receive an SMS password and this password will be used in the banks' website and after matching the password, the user will be allowed the entry.

3. **Biometrics**:-Based on physical or physiological characteristics a person will be identified, for example-figure prints. Among the available options it is the best and accurate method. But it is difficult to implement on large scale.

4. **Digital Signature Certificate**:-Digital certificates can be stored and transported on smart cards or USB tokens. There are number of issues with deployment of digital signatures.


www.southindianbank.com
YOUR DREAM VEHICLES ARE DIFFERENT.
SO ARE OUR VEHICLE LOAN SCHEMES.
TAILORED TO SUIT THE NEEDS OF:
| SALARIED CLASS | BUSINESS PEOPLE | NEXT GEN
| AGRICULTURISTS | NRIs | SENIOR CITIZENS
blackswanindia.com
*Terms & conditions apply
| Low Interest Rates | Easy Processing | Enhanced Eligibility
SOUTH INDIAN Bank
Experience Next Generation Banking
The South Indian Bank Ltd., Regd. Office, SIB House,P.B. No. 28, Thrissur, Kerala, PIN-680 001
Ph: 0487 2420020, Fax: 0487 2426187, Toll Free (India): 1800-843-1800, 1800-425-1809 (BSNL)
Email: sibcorporate@sib.co.in | CIN : L65191KL1929PLC001017
South Indian Bank is a member of BCSBI and is committed to treat customers in a fair, transparent and non-discriminatory manner.
http://www.facebook.com/thesouthindianbank

www.southindianbank.com

SHAKE TO TRANSFER MONEY AND DO MUCH MORE.

SIB MIRROR
REFLECTION OF SOUTH INDIAN BANK

Never-before features on a smart banking app:

Shake to transfer funds | Shake to know balance | Click to share your account information | Gesture support for menu access* | Menu navigation using voice recognition* | Pattern lock

OTHER FEATURES

Calculators | Forex Rates | SIB Locator | My Account (only for SIB account holders) | Deposit Rates | Apply for Deposits and Loans | Contact Us | About Us

*Handset specific

THE SMART WAY TO BANK WITH SOUTH INDIAN BANK.
DOWNLOAD SIB MIRROR ON YOUR SMARTPHONE NOW.

Android | i-Phone | Windows Phone | Blackberry

blackswanindia.com

The South Indian Bank Ltd., Regd. Office, SIB House, P.B. No. 28,
Thrissur, Kerala, PIN-680 001, Ph: 0487 2420020, Fax: 0487 2426187,
Toll Free (India): 1800-843-1800, 1800-425-1809 (BSNL),
Email: sibcorporate@sib.co.in | CIN : L65191KL1929PLC001017

http://www.facebook.com/thesouthindianbank

SOUTH INDIAN Bank
Experience Next Generation Banking

South Indian Bank is a member of BCSBI and is committed to treat customers in a fair, transparent and non-discriminatory manner.