सत्यमेव जयते

रक्षा मंत्रालय
MINISTRY OF
DEFENCE

CISO NEWSLETTER

Volume 1, Issue 4

FOREWORD

Nearly all aspects of life of a common person are digitized today. One such prime facet which directly impacts a person is banking/ financial services. Digitization of banking/ financial services has revolutionized the banking experience of a user offering a host of conveniences and possibilities. Online banking, debit/ credit cards, ATMs, e-Wallets etc has made handling cash/ money seamless and hassle free.

There are large number of fraudsters lurking out there, looking for victims in naive and untrained users. Reports of online financial fraud and incidents which have caused considerable loss to users keep surfacing every now and then. It is however interesting to know that securing one's online transactions, debit/credit card, e-Wallets etc. is not a rocket science. Adhering to simple ground rules and a disciplined approach can secure one's digital financial activities. This edition of newsletter touches upon this ever important cyber security aspect and presents user level security tips to secure their digital payments.

Feedback and suggestions regarding CISO newsletter are welcome.

V Anandarajan
Joint Secretary

CISO NEWSLETTER

DIGITAL PAYMENTS

Digital Payments are any payments made by using digital instruments. In digital payment, the payer and the payee, both use electronic modes to send and receive money. No hard cash is used.

Types of Digital Payments

i) Banking Cards
ii) UPI
iii) Internet Banking
iv) Mobile Wallets
v) Point of Sale (PoS)

BANK CARDS

A bank card is any card issued against a depository account, such as an ATM card or a debit card/ credit card. These are issued by financial institutions, such as a bank, to a customer that enables its owner (the cardholder) to access the funds in the customer's designated bank accounts, or through a credit account and make payments by electronic funds transfer and access automated teller machines (ATMs).

There are a number of types of payment/ bank cards, the most common being credit cards and debit cards. However, based on the technology being used in the cards, they can be further categorized under the following types:-

(a) Magnetic Strip Cards
(b) Chip Card
(c) Contactless Card
(d) Chip & Pin card

CISO NEWSLETTER

CATEGORISATION OF BANKING CARDS

The **Magnetic Strip Card** allows customer to perform transaction by using the information loaded in the layers of magnetic strip.

AUTHORIZED SIGNATURE
NOT VALID UNLESS SIGNED
4000 1234 5678 9010 123

A **Chip Card** creates a unique transaction code during payments that can not be used again.

CATEGORISATION OF BANKING CARDS

Contactless Cards allow transactions by waving or tapping cards at an EMV enabled terminal.

A Chip and Pin Card is a card in which data is embedded in a micro chip and requires the customer to enter PIN to complete the transaction.

CISO NEWSLETTER

UPI

A **Unified Payment Interface (UPI)** is a smart phone application which allows users to transfer money between bank accounts. It is a single-window mobile payment system developed by the National Payments Corporation of India (NPCI). It eliminates the need to enter bank details or other sensitive information each time a customer initiates a transaction.

INTERNET BANKING

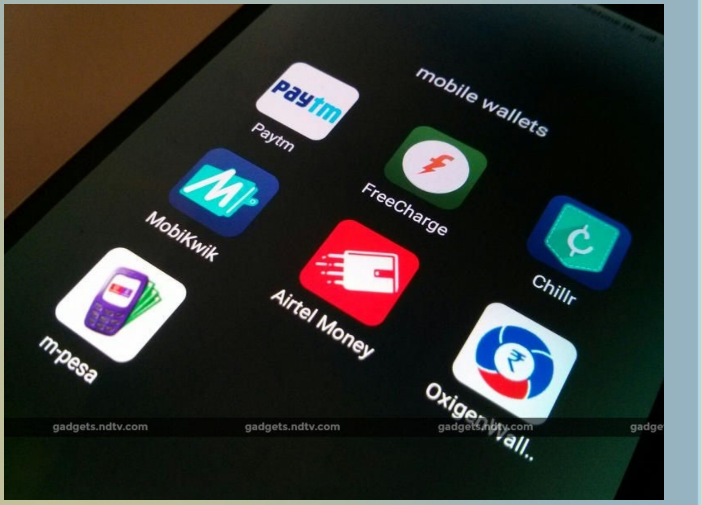
Internet banking allows a user to conduct financial transactions via the internet. Online banking offers customers almost every service traditionally available through a local branch including deposits, transfers, and online bill payments.

shutterstock.com • 552334819

CISO NEWSLETTER

MOBILE WALLETS

The **Mobile Wallet** is an app that can be installed on a smart phone or it is an existing built-in feature of a smart phone which is used for make online transactions.



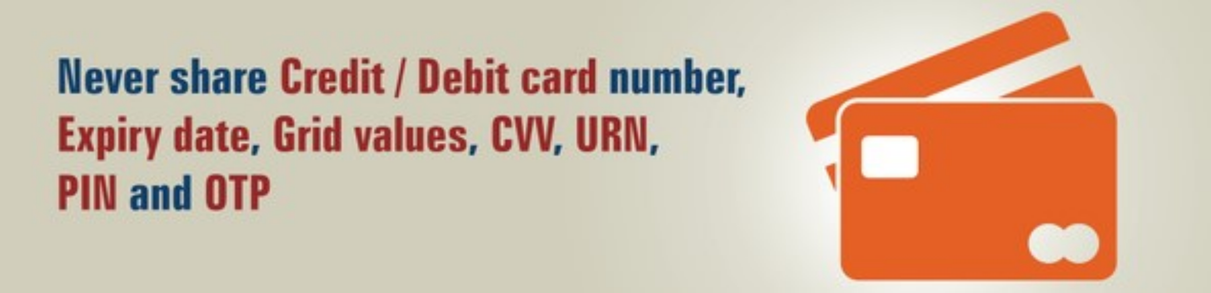
POINT OF SALE DEVICES

A **Point of Sale Device** is a combination of PoS Hardware and PoS software to create a PoS terminal for processing a transaction and payment.

CISO NEWSLETTER

GENERAL PRECAUTIONS WHILE USING BANKING CARDS

- Never keep your credit/ debit card and the PIN at one place.
- Do change your card PIN every Quarterly.
- Do not share PIN, CVV number and card details with anybody.



Never share Credit / Debit card number, Expiry date, Grid values, CVV, URN, PIN and OTP

- Do not tell OTP to anyone and bank will never call for it.
- When you dispose a card for renewal/up gradation, please make sure to cut it diagonally before disposal.

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

CISO NEWSLETTER

PRECAUTIONS WHILE USING PAYMENT CARDS AT MERCHANT LOCATIONS

- Always keep an eye that how the vendor swipes your card and make sure transactions happen in your presence.

- Do not throw away the transaction receipt when you are done with it. Tear it or shred it. Dumpster divers are known to swift through garbage bags meticulously and retrieve all your card related information that can then be used to conduct unauthorized purchases, especially over the internet.

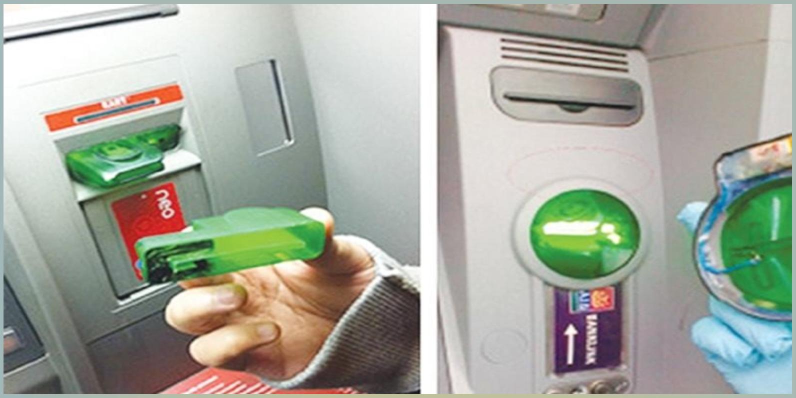
- Always retain the transaction receipt for comparing against the card statement that you receive at the end of the month. Most people throw this away and do not match against the amount charged in the statement.

- 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.

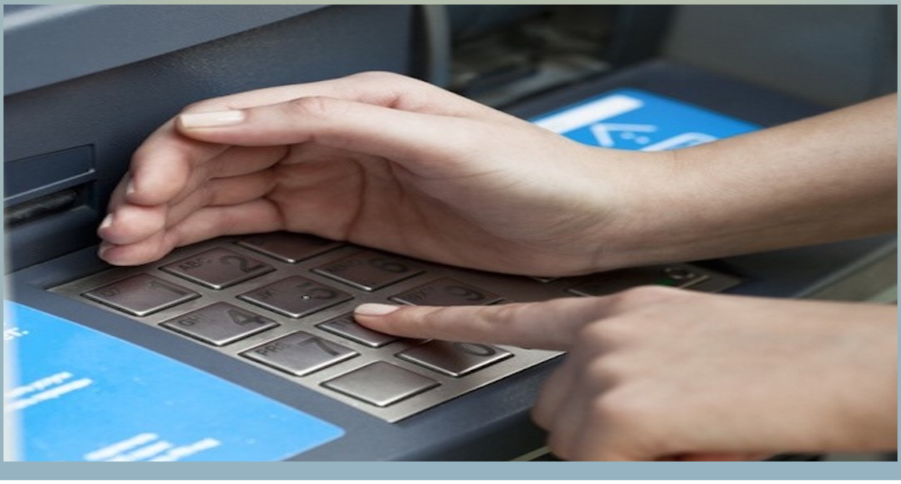
CISO NEWSLETTER

PRECAUTIONS WHILE USING PAYMENT CARDS AT ATMs

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



- Ensure that your transaction is ended/completed at ATM machine before leaving the premises.
- 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.

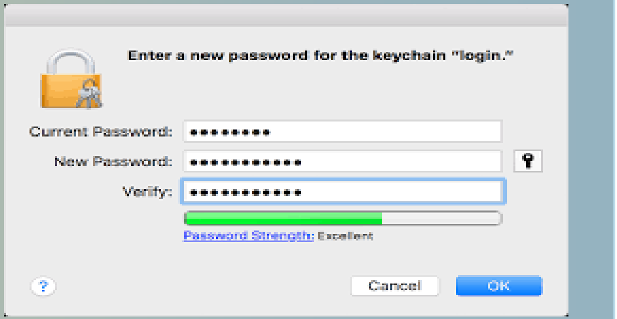


CISO NEWSLETTER

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 using e-wallets. Additional layers of security provided by these devices should be used.



Enter a new password for the keychain "login."

Current Password: ••••••••

New Password: ••••••••••••

Verify: ••••••••••••

Password Strength: Excellent

Create a Unique Password for e-Wallet:

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

CISO NEWSLETTER

BEST PRACTICES FOR USERS TO REMAIN SAFE WHILE USING E-WALLETS

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 Wi-Fi connections identified as ‘WPA2’ requiring strong passwords should be used.

Install e-Wallet 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).

CISO NEWSLETTER

BEST PRACTICES FOR USERS TO REMAIN SAFE WHILE USING E-WALLETS

Stay vigilant and aware of cell phone's network connectivity status and register for Alerts through SMS and emails:

The user should not switch off his cell phone 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.

CISO NEWSLETTER

BEST PRACTICES FOR USERS TO REMAIN SAFE WHILE USING E-WALLETS

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.

SMART TIPS WHILE USING INTERNET BANKING SERVICES

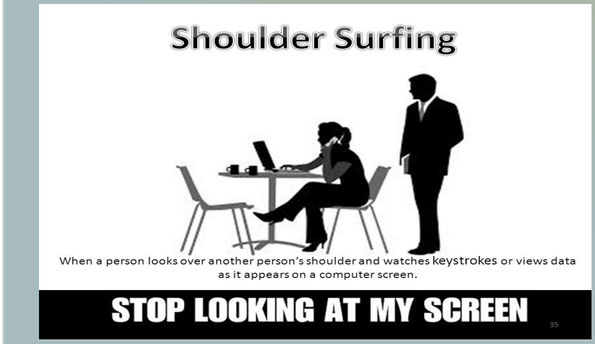
COMPUTERS AND MOBILE PHONES

Protect your computer and mobile phone for logging into your internet banking.

Avoid using public computers or public Wi-Fi to access internet banking services.

LOGIN PROCESS

Beware of any unusual login screen or process (e.g. a suspicious pop-up window or request for providing additional personal information) and whether any one is trying to peek at your password.

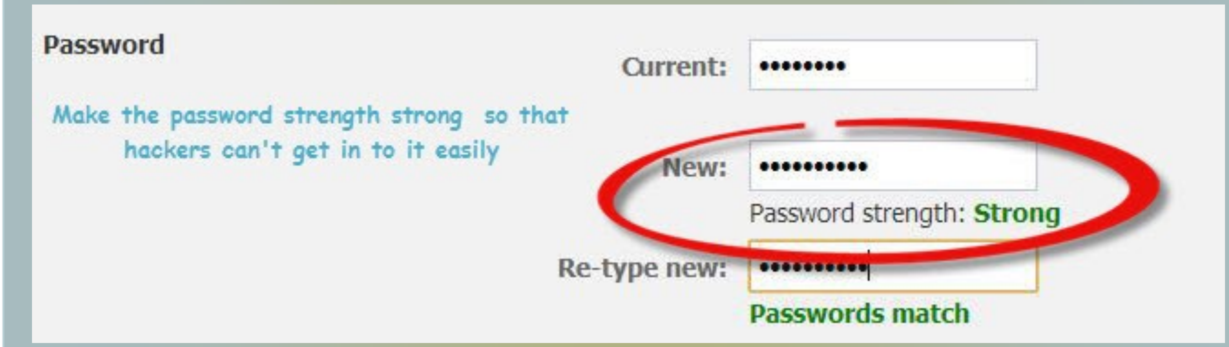

Shoulder Surfing
When a person looks over another person's shoulder and watches keystrokes or views data as it appears on a computer screen.
STOP LOOKING AT MY SCREEN
35

CISO NEWSLETTER

SMART TIPS WHILE USING INTERNET BANKING SERVICES

LOGIN PASSWORDS

Set a password that is difficult to guess and different from the ones used for other accounts/services.



Password

Make the password strength strong so that hackers can't get in to it easily

Current: •••••••••

New: •••••••••••

Password strength: Strong

Re-type new: •••••••••••

Passwords match

The login password should be changed regularly and should never be stored on computers, mobile phones or placed in plain sight.

MESSAGES FROM BANKS

Check your bank's SMS messages and other messages in a timely manner and verify your transaction records.

Inform your bank immediately in case of any suspicious situations.

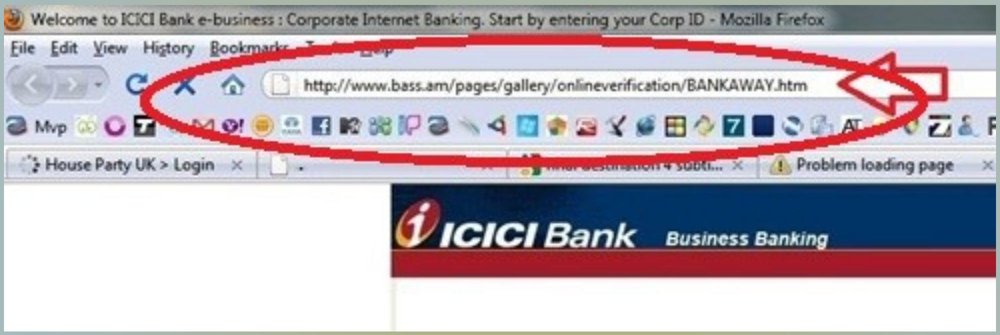
Banks will not ask for any sensitive personal information through phone calls or emails.

CISO NEWSLETTER

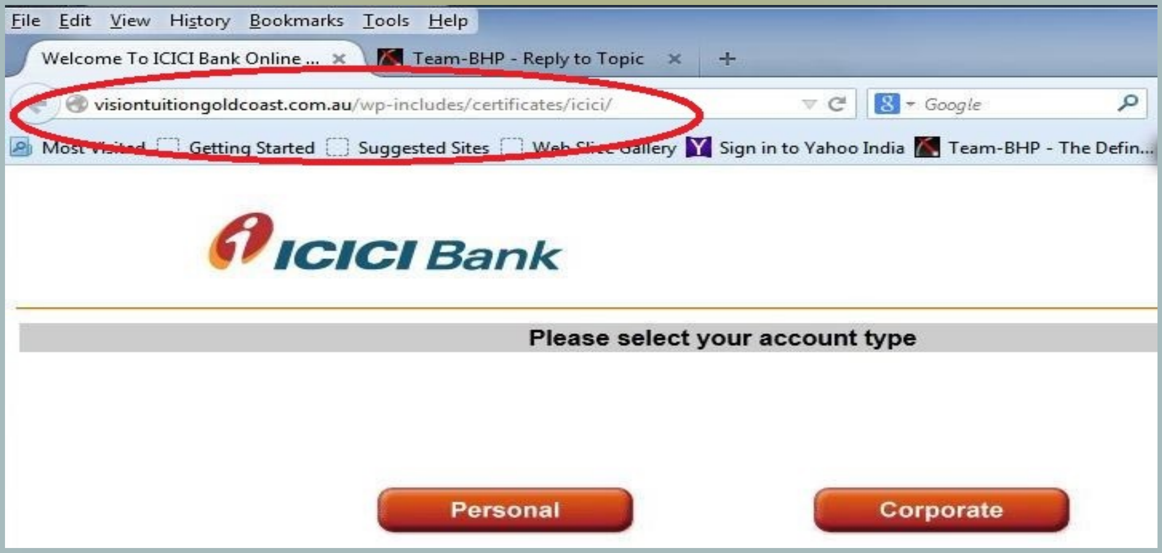
SMART TIPS WHILE USING INTERNET BANKING SERVICES

BANKING WEBSITES AND APPS

Internet banking should be accessed by entering the bank's website address directly or using a bookmark or internet banking mobile application.


Welcome to ICICI Bank e-business : Corporate Internet Banking. Start by entering your Corp ID - Mozilla Firefox
File Edit View History Bookmarks
http://www.bass.am/pages/gallery/onlineverification/BANKAWAY.htm
House Party UK > Login
Problem loading page
ICICI Bank Business Banking

Never access your bank website or provide your personal information through any hyperlinks or attachments embedded in emails or from websites.


File Edit View History Bookmarks Tools Help
Welcome To ICICI Bank Online ...
Team-BHP - Reply to Topic
visiontuitiongoldcoast.com.au/wp-includes/certificates/icici/
Google
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery
Sign in to Yahoo India
Team-BHP - The Defin...
ICICI Bank
Please select your account type
Personal
Corporate

CISO NEWSLETTER

REFERENCES

1. https://infosecawareness.in/home/index.php
2. https://cert-in.org.in/
3. Cyber Security Handbook for Digital Financial Transactions by CDAC/ Information Security Education & Awareness (ISEA)

Incidents related to Cyber Crime in New Delhi may be reported at the following

Website.
http://www.cybercelldelhi.in/

For online registration of complaints, visit the url http://205.147.111.155:84/

HELPDESK

CISO Office	:	011-23018232
Cyber Cell	:	011-23794783
E-Mail ID	:	cybercell-mod@nic.in

Concept	**:**	**Wg Cdr Bhattacharya** **Lt Col VK Jha**
Content	**:**	**Lt Cdr Riazuddin**
Prepared by	**:**	**Sgt Sukumar Reddy**