certin Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0084

Secure payment through RuPay card

Original Issue Date: December 21, 2016

Description

The India Pay scheme renamed RuPay(i.e. rupee and payment), is an Indian domestic card scheme initiative by National Payments Corporation of India (NPCI). It is very similar to international cards such as Visa/Master. It is an alternative to the MasterCard and Visa card schemes to consolidate and integrate various payment systems in India. RuPay has certified 29 major banks in India to accept the RuPay card at their respective PoS terminals located at different merchant locations.

NPCI has rolled out its chip card for high security transactions using EMV (Europay, MasterCard and Visa) chip technology, which is a global standard for debit and credit cards. RuPay chip cards have an embedded microprocessor circuit containing information about the card holder and because transactions are PIN-based rather than signature-based.

Banks in India are authorized to issue RuPay debit cards to their customers for use at ATMs, PoS terminals, and e-commerce websites. In addition to the ATMs and PoS terminals, RuPay cards are accepted online on e-commerce websites with the same PIN which they use for ATM transactions.

Threats to RuPay card

- **Phishing/Smishing/Vishing Attack:** An attacker attempts phishing on to a ecommerce websites/mobile phone either through SMS (Short Message Service),text message, telephone call, fax, voicemail etc. or through phishing or malicious software with a purpose to convince the recipients to share their sensitive or personal information.
- **Channel breaking attack (CBA):** CBA involves intercepting the communication between the client side and the banking server, by masquerading as the server to the client and vice versa.
- **MiTB attack:** 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.
- **Outdated OSs and Nonsecure Network Connections:** Risk factors such as out-dated operating system versions, use of nonsecure Wi-Fi network in mobile devices allow cybercriminals to exploit an existing online banking session to steal funds and credentials.
- **Unauthorized** usage of a credit card as a result of it being lost or stolen.
- **Counterfeit:** duplicating/cloning legitimate credit cards which are then used for fraudulent activities.

Best Practices for Users

- Install anti-spyware security software against those programs that monitor, record and extract the personal information you type in your PC (passwords, card numbers, ID numbers, etc.)
- Install personal firewalls to protect your PC against unauthorized access by hackers
- Keep your operating system and internet browser up to date, checking for and downloading new versions/security enhancements from the vendor's web site
- Do give the mailing address, residential or office address, where you are sure as to who will receive the Card/PIN
- Inform the Bank immediately about change in your mailing address to ensure correct delivery of your Card/PIN
- Before using Cards, please ensure that there are no strange objects in the insertion panel of the ATMs/PoS
- Cover the PIN pad while entering PIN at ATMs/PoS
- 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
- Shred anything that contains credit card number written on it. (bills etc)
- Notify credit/debit card issuers in advance for change of address
- Do not accept card received directly from bank in case if it is damaged or seal is open
- Do not write PIN number on credit/debit card or on a paper which you carry along with the card.
- Do not disclose Credit Card Number/ATM PIN to anyone.
- Do not hand over the card to anyone, even if he/she claims to represent the Bank.
- In case of any suspected transactions or loss of cards, contact the service provider / bank immediately
- When you dispose your Card at the time of renewal/up gradation, please make sure that you cut it diagonally before disposal
- Please keep your Card in a safe place. Treat it as carefully as you would treat your cash
- Please make sure you conduct any ATM transaction in complete privacy
- Please remember to take your Debit Card back after completing your ATM transaction
- Please sign your Debit Card as soon as you get it
- Please check your Card periodically to make sure it is not missing
- Please do not provide any financial/personal/Debit Card related information to unknown websites or respond to emails seeking such information

- 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.
- Ignore and delete immediately suspicious fraudulent (phishing, spoof,hoax) e-mails that appear to be from Bank, asking you to urgently click a link to a fraudulent (spoof) website that tries to mimic the Bank's site and to lure you into giving out your sensitive personal information (PIN, account or card numbers, personal identification information etc.)
- Use an online verification scheme(e.g. OTP etc.) for online purchases
- 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.

References

NCPI
http://www.npci.org.in/RuPay_faqs.aspx
https://en.wikipedia.org/wiki/RuPay

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India