Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0065

Security of Electronic-wallets

Original Issue Date: November 30, 2016

Systems Affected

- Electronic-Wallets

Description

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

1. 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;

1. Avoid falling prey to social engineering tricks: Financial service providers 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.
2. 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.

2. 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 Padlock 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.

3. Malware Attacks

Malware attacks on apps have threatened the safety of users 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:

1. 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.
2. 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

- Enable Passwords On Devices: Strong passwords should be enabled on the users 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 provider¿s contract terms and conditions.

References

https://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf
https://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062
http://www.welivesecurity.com/2015/03/03/10-tips-protecting-virtual-bitcoin-wallet/

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