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

CERT-In Advisory CIAD-2016-0070

Securing Mobile Banking

Original Issue Date: December 06, 2016

Description

The increasing usage of Smartphones 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.

Threats to Mobile Banking

1. **Mobile Banking Malwares :** There have been incidents that involved sophisticated virus infecting bank¿s mobile apps users to steal password details and even thwart 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.

2. **Phishing/Smishing/Vishing Attack :** An attacker attempts phishing on to a mobile phone through SMS (Short Message Service),text message, telephone call, fax, voicemail 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.

3. **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.

4. **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.
    - 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 users 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 alternately 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.

Workaround

- Restricting management access to only trusted management networks and hosts where a legitimate management login would be permitted.

- Enable router logging and review it periodically.

References

https://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062
http://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0069

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