Digital Payments Safety Initiative by NPCI

Press Release February 18, 2019

Mumbai: National Payments Corporation of India is at the forefront of driving digital payments to deliver a simple, secure and seamless experience for consumers. With the widespread acceptance and growth of Digital payments it is paramount that consumers also learn safety aspects of any new ecosystem. NPCI started the process of consumer safety within the apps with various security controls.

RBI has recently issued Advisory (Alert 1/2019) dated 14th Feb'19 pertaining to new modus operandi to commit fraud in Digital Payment Ecosystem using Remote screen access apps. NPCI is committed to consumer safety and reiterates its commitment to support the cause stated by RBI in letter and spirit. Recently, this new type of fraud has been identified by NPCI only and proactively informed to the regulator and other authorities.

Modus Operandi (Remote Screen Access)

- Fraudster would lure the victim on some pretext to download an app called 'AnyDesk' from Playstore or Appstore.
- The app code (9-digit number) would be generated on victim's device which the fraudster would ask the victim to share.
- Once fraudster inserts this app code (9-digit number) on his device, he would ask the victim to grant certain permissions which are similar to what are required while using other apps.
- Post this, fraudster will gain access to victim's device.
- Further the mobile app credential is vished from the customer and the fraudster then can carry out transactions through the mobile app already installed on the customer's device.

Notably the threat of this modus operandi applies to all applications (Payment/Banking/Wallets/Social Media) installed on the victim's mobile device. Once access is granted by the victim, fraudster can not only initiate financial transactions but can also place online shopping orders or book rail/air tickets, etc. using the apps available on the victim's phone or even steal any information stored in the mobile phone. While number of such fraud cases are few (5 cases reported so far), we are vigilant and urge consumers to be careful.

Bharat Panchal, Head of Risk Management, NPCI says, "While NPCI is continuously working towards enhancing security of its products & services from such attacks, this type of frauds can be better prevented by consumer education. The entire ecosystem including Banks & Fintech companies have to work collectively towards creating awareness & educating customers to refrain from sharing their account/card credentials, OTP/PIN and/or giving access to their mobile handsets to unscrupulous persons through such remote screen access apps. UPI platform is fully secure and is also 2FA enabled. NPCI in its endeavour to safeguard the UPI ecosystem will continue to proactively monitor the fraud space and help implement control measures wherever required."

Taking this ahead, NPCI started with the Consumer Safety & Awareness program leveraging the mass media vehicles like newspapers and radio. Last week, NPCI started a consumer content sourcing initiative STOP. THINK. ACT on twitter to gather creative ideas from consumers to educate them. This is one of the kind initiative to co create content along with consumers, in true sense "for the consumers, by the consumers"

About NPCI: National Payments Corporation of India (NPCI) was set up in 2009 as the central infrastructure for various retail payment systems in India and was envisaged by the Reserve Bank of India (RBI) as the payment utility in the country. From a single service of switching of interbank ATM transactions through National Financial Service, the range of services has grown to Cheque Truncation System, National Automated Clearing House (NACH), Aadhaar Enabled Payment System (AePS), USSD based *99#, RuPay card, Immediate Payment Service (IMPS), Bharat Interface for Money - Unified Payments Interface (BHIM UPI), BHIM Aadhaar, National Electronic Toll Collection (NETC) and Bharat BillPay.

Media contact: corporate.communications@npci.org.in
Adfactors –
Mihir Dani – mihir.dani@adfactorspr.com – 7738012080
Priyadarshini Sinha – priyadarshini.sinha@adfactorspr.com – 999627610
Shruti Nitesh – shruti.nitesh@adfactorspr.com - 8108000974