डिजिटल भुगतान में धोखाधड़ी के मामले

*65. **श्री नरेश अग्रवाल** : क्या **इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री** यह बताने की कृपा करेंगे किः

(क) क्या यह सच है कि डिजिटल भुगतान में धोखाधड़ी के मामले बढ़ रहे हैं, यदि हां, तो इसके क्या कारण हैं;

(ख) सरकार द्वारा डिजिटल सुरक्षा के संबंध में क्या-क्या कदम उठाए गए हैं; और

(ग) डिजिटल सुरक्षा के संबंध में चन्द्रबाबू नायडु समिति द्वारा क्या-क्या सुझाव दिए गए थे?

इलेक्ट्रॉनिकी ऑर सूचना प्रौद्यागिकी मंत्री (श्री रवि शंकर प्रसाद): (क) से (ग) एक विवरण सभा पटल पर रख दिया गया है।

विवरण

(क) वर्ष 2015-15 और 2016-17 के दौरान क्रेडिट कॉर्ड, एटीम/डेबिट कार्ड, इंटरनेट बैंकिंग को शामिल करते हुए धोखाधड़ी के मामलों की संख्या निम्नानुसार हैः

2015-16	2016-17
16468	13653

ई-वॉलेट सहित प्रीपेड पेमेंट इंस्ट्रूमेंट (पीपीआई) के लिए भारतीय रिज़र्व बैंक (आरबीआई) ने धोखाधड़ी वाले लेनदेनों का अनंतिम डाटा एकत्र करना शुरू कर दिया है। डाटा के अनुसार मार्च, अप्रैल और मई, 2017 के लिए धोखाधड़ी वाले लेनदेनों की संख्या कुल लेनदेनों की कुल संख्या के 0.005% से 0.007% के बीच है।

भारतीय कम्प्यूटर आपात प्रक्रिया दल (सर्ट-इन) को रिपोर्ट की गई घटनाओं के अनुसार नवम्बर, 2016 से जून, 2017 के दौरान 19 वित्तीय संगठनों को प्रभावित करनेवाली फिशिंग की 40 घटनाएं और एटीएम, बिक्री बिंदु (पीओएस) प्रणालियों और एकीकृत भुगतान अंतरापृष्ठ (यूपीआई) को प्रभावित करने वाली 10 घटनाएं रिपोर्ट की गई हैं।

डिजिटल भुगतान को बढ़ावा देने के भाग के रूप में सरकार यह सुनिश्चित करने के लिए कई कदम उठा रही है कि धोखाधड़ी को न्यूनतम किया जा सके और यहां तक जब इस प्रकार की कोई घटना घटित होती है, तो तत्काल निर्वारक कार्रवाई की जाती है।

(ख) डिजिटल भुगतान प्रणाली को सुरक्षित करने के लिए सरकार द्वारा उठाए गए कदम अनुबंध में नीचे दिए गए हैं (नीचे देखिए)।

(ग) आंध्र प्रदेश के मुख्यमंत्री माननीय श्री चन्द्रबाबू नायडू की अध्यक्षता में डिजिटल भुगतान पर मुख्यमंत्रियों की समिति ने अपनी अंतरिम रिपोर्ट में डिजिटल भुगतान सुरक्षा पर निम्नलिखित सुझाव दिए हैंः

(i) सचिव, एमईआईटीवाई और डीओटी की अध्यक्षता में गठित स्थायी समिति को निजी क्षेत्र के सेवा प्रदाताओं, बैंकों और आरबीआई के साथ परामर्श से एनपीसीआई की सुरक्षा प्रणाली को सुदृढ़ करने पर ध्यान केंद्रित करना चाहिए।

(ii) सरकार को धोखाधड़ी आदि के फलस्वरूप डिजिटल भुगतानों में होने वाली हानि की प्रतिपूर्ति के लिए कोई बीमा योजना तैयार करनी चाहिए जिससे कि डिजिटल भुगतान अपनाने में आम जनता की दुविधा को दूर किया जा सके। योजना के अंतर्गत छोटे दुकानदारों, किसानों आदि जैसे सुभेद्य वर्गों को बीमित करने के लिए कम राशि वाली लेनदेनों को लक्ष्य बनाया जाना चाहिए।

(iii) डिजिटल भुगतान के लिए एक अलग प्राधिकरण की स्थापना की जाए। यह प्राधिकरण इस क्षेत्र में हो रहे विकास, नियामक मुद्दों, सुरक्षा संबंधी पहलुओं आदि का पर्यवेक्षण करने के लिए उत्तरदायी होगा। इस निकाय के गठन के लिए आवश्यक विधायी और नीतिगत परिवर्तन किए जाएं।

अनुबंध

डिजिटल भुगतान प्रणाली की सुरक्षा के लिए सरकार द्वारा उठाए गए कदम

1. भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) डिजिटल प्रौद्योगिकियों का सुरक्षित इस्तेमाल सुनिश्चित करने के लिए उपयुक्त उपाय करने हेतु पणधारकों के बीच जागरूकता पैदा करने के लिए नवीनतम साइबर खतरों के संबंध में नियमित आधार पर चेतावनी और परामर्शी निदेश (एडवाइजरी) और प्रति उपाय जारी करता है। डिजिटल भुगतान सुरक्षित करने के लिए प्रयोक्ताओं और संस्थानों हेतु सुरक्षा उपायों के संबंध में अब तक ऐसे 25 परामर्शी निदेश (एडवाइजरी) जारी किए हैं।

2. देश में प्रीपेड पेमेंट इंस्ट्रूमेंट (पीपीआई) जारी करने वाले सभी प्राधिकृत निकायों/बैंकों को भारतीय रिज़र्व बैंक के माध्यम से भारतीय कम्प्यूटर आपात प्रतिक्रिया दल द्वारा यह सलाह दी गई है कि वे भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) के सूचीबद्ध लेखापरीक्षकों द्वारा प्राथमिकता आधार पर लेखापरीक्षा कराएं और उसके पश्चात् लेखापरीक्षा रिपोर्ट के निष्कर्षों का अनुपालन करें तथा सुरक्षा श्रेष्ठ पद्धतियों का कार्यान्वयन सुनिश्चित करें।

3. डिजिटल भुगतान सेवाएं उपलब्ध कराने वाले सभी संगठनों को साइबर सुरक्षा की घटनाओं के बारे में भारतीय कंप्यूटर आपत प्रतिक्रिया दल को शीघ्रता से रिपोर्ट करना अनिवार्य किया गया है।

4. सरकारी और महत्वपूर्ण क्षेत्रों के संगठनों की साइबर सुरक्षा की स्थिति और तैयारी का मूल्यांकन करने में उन्हें सक्षम बनाने के लिए नियमित रूप से साइबर सुरक्षा मॉकड्रिल संचालित की जा रही हैं। अब तक भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) द्वारा इस प्रकार की 15 मॉकड्रिल संचालित की गई हैं जिनमें विभिन्न क्षेत्रों के 148 संगठनों ने भाग लिया।

5. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) द्वारा डिजिशाला जागरूकता अभियान के अंतर्गत साइबर सुरक्षा जागरूकता सत्रों का आयोजन किया जाता है।

6. सरकार ने देश में संक्रमित प्रणालियों का पता लगाने और उन्हें ठीक करने के लिए साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग एण्ड मालवेयर एनालिसिस सेंटर) स्थापित किया है। यह परियोजना इंटरनेट सेवा प्रदाताओं और उद्योग जगत के साथ समन्वय से शुरू की गई है।

7. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) ने डिजिटल भुगतान प्रणालियों की सुरक्षा के संबंध में बैंकों, इंटरनेट सेवा प्रदाताओं (आईएसपी) और प्रीपेड पेमेंट इंस्ट्रूमेंट (पीपीआई) के लिए 2 कार्यशालाएं आयोजित की हैं।

8. सरकार ने अनुप्रयोगों और अवसंरचना की सुरक्षा के लिए मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए सामान्य दिशानिर्देश और अनुपालन के लिए उनकी प्रमुख भूमिकाओं तथा जिम्मेदारियों से संबंधित निर्देश जारी किए हैं।

9. सर्ट-इन वर्तमान खतरा परिदृश्य और प्रतिउपायों के बारे में जागरूक बनाने के लिए सरकार तथा महत्वपूर्ण क्षेत्र के संगठनों के सीआईएसओ सहित आईटी/साइबर सुरक्षा पेशेवरों के लिए नियमित रूप से साइबर सुरक्षा प्रशिक्षण सचालित करता है। इसके अलावा, सर्ट-इन ने पणधारक संगठनों के लिए डिजिटल भुगतान प्रणालियों की सुरक्षा पर एक कार्यशाला भी आयोजित की है, जिसमें 110 प्रतिभागियों ने भाग लिया।

10. भारतीय रिज़र्व बैंक ने रिपोर्ट की गई किसी भी मुख्य घटना का समाधान करने के लिए साइबर आपदा प्रबंधन ग्रुप की स्थापना की है जिसमें घटनाओं का सामना करने और उनसे भरपाई के तरीके भी सुझाए गए हैं।

11. भारतीय रिज़र्व बैंक के अधीन बैंकिंग पर्यवेक्षण विभाग सर्ट-इन के सहयोग से आभासी परिदृश्यों के आधार पर बैंकों की तैयारी का जायज़ा लेने के लिए साइबर सुरक्षा तैयारी परीक्षण करता है।

12. भारतीय रिज़र्व बैंक ने देश में प्रीपेड इंस्ट्रूमेंट (पीपीआई) जारी करने वाले सभी प्राधिकृत संगठनों/बैंकों के लिए सुरक्षा और जोखिम उन्मूलन संबंधी उपायों पर 9 दिसम्बर, 2016 को एक प्ररिपत्र जारी किया है।

13. भारतीय रिज़र्व बैंक फिशिंग हमलों पर तथा फिशिंग हमलों का सामना करने के लिए निवारक/संसूचक उपायों पर सभी व्यावसायिक बैंकों को परिपत्र/सलाह जारी करता है। बैंक भी अपने प्रयोक्ताओं के साथ इसका अनुपालन कर रहे हैं।

14. भारतीय रिज़र्व बैंक ने वर्ष 2015 में एक साइबर सुरक्षा और आईटी परीक्षण (सीएसआईटीई) सैल की स्थापना की है।

15. भारतीय रिज़र्व बैंक ने साइबर सुरक्षा के विभिन्न पक्षों संबंधी श्रेष्ठ पद्धतियों को शामिल करते हुए 2 जून, 2016 को बैंकों में साइबर सुरक्षा ढांचे पर एक व्यापक परिपत्र जारी किया है।

16. भारतीय रिज़र्व बैंक ने भारत में प्रीपेड इंस्ट्रूमेंट (पीपीआई) जारी करने और उनके प्रचालन पर मसौदा मास्टर दिशानिर्देश तैयार किए हैं और 20 मार्च, 2017 को इस पर जनता की टिप्पणियां आमंत्रित की गई हैं।

Cases of fraud in digital payments

†*65. SHRI NARESH AGRAWAL: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that the number of cases of fraud in digital payments have increased, if so, the reasons therefor;

(b) the steps taken by Government in respect of digital security; and

(c) the suggestions made by Chandra Babu Naidu Committee on digital security?

THE MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI RAVI SHANKAR PRASAD): (a) to (c) A Statement is laid on the Table of the House.

Statement

(a) The number of cases of frauds involving credit cards, ATM/Debit cards and Internet banking during the year 2015-16 and 2016-17 are as follows:

2015-16	2016-17
16468	13653

For prepaid payments instruments including e-wallets, Reserve Bank of India (RBI) has started maintaining provisional data of fraudulent transactions. According to the data for March, April and May 2017, the number of fraudulent transactions is between 0.005% to 0.007% of the total number of transactions.

As per incidents reported to the Indian Computer Emergency Response Team (CERT-In), 40 phishing incidents affecting 19 financial organisations and 10 incidents affecting ATMs, Point of Sales (POS) systems and Unified Payment Interface (UPI) have been reported during November 2016 to June 2017.

As part of promotion of digital payments, Government is taking several steps to ensure that frauds are minimised and even when an incident of this nature takes place, corrective action is immediately taken.

† Original notice of the question was received in Hindi.

(b) The steps taken by Government to secure digital payment system are given in the Annexure (*See* below).

(c) The Committee of Chief Ministers on Digital Payment, chaired by Chief Minister of Andhra Pradesh Shri Chandrababu Naidu, has in its Interim Report suggested the following on Digital Payment security:

(i) The Standing Committee formed under Chairmanship of Secretary, MeitY and DoT should focus on strengthening NPCI security system, consultations with private service providers, banks and RBI.

(ii) Government should come out with an insurance scheme to cover losses incurred in digital transactions on account of fraud, etc. In order to address the apprehension of general public in adopting digital payments. The scheme should target low ticket transactions to cover the vulnerable sections like small merchants, farmers etc.

(iii) A separate Authority may be set up for Digital Payments. The Authority will be responsible for overseeing sector development, regulatory issues, security aspects, etc. Necessary legislative and policy changes may be effected to create this body.

Annexure

Steps taken by Government to secure digital payment system

1. CERT-In issues alerts and advisories regarding latest cyber threats/ vulnerabilities alongwith countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. Regarding securing digital payments, 25 advisories have been issued for users and institutions.

2. In addition, all authorised entities/banks issuing PPIs in the country have been advised by CERT-In through the Reserve Bank of India to carry out security audit by the empanelled auditors of CERT-In on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

3. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

4. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government

and critical sectors. Till date, 15 such drills have been conducted by the Indian Computer Emergency Response Team (CERT-In) involving 148 organizations from different sectors including Finance sector.

5. Cyber security awareness sessions are conducted by Ministry of Electronics and Information technology (MeitY) under the Digishala Awareness Campaign.

6. Government has established Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.

7. MeitY has organised 2 workshops for banks, Internet Service Providers (ISPs) and Prepaid Payment Instruments (PPIs) issuing entities regarding security of digital payments systems.

8. Government has issued general guidelines for Chief Information Security Officers (CISOs) for securing applications and infrastructure and their key roles and responsibilities for compliance.

9. CERT-In is regularly conducting cyber security trainings for IT / cyber security professionals including CISOs of Government and critical sector organisations to give an exposure on current threat landscape and countermeasures. In addition, CERT-In has also conducted a workshop on security of digital payments systems for stakeholder organisations covering 110 participants.

10. RBI has set up a Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents.

11. Department of Banking Supervision under RBI, with the help of CERT-In, conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios.

12. RBI has issued a circular on 9th December 2016 for security and risk mitigation measure for all authorised entities / banks issuing Prepaid Payment Instrument (PPI) in the country.

13. RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. Banks have also been following the same with their users.

14. RBI has set up a Cyber Security and IT Examination (CSITE) cell in 2015.

15. RBI has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security.

16. RBI has prepared draft Master Directions on issuance and operations of Prepaid Payments Instruments in India and on 20 March 2017 has invited public comments on the same.

श्री नरेश अग्रवालः महोदय, हम मंत्री जी के साथ बैठकर डिस्कस कर लेंगे और समय रह नहीं गया है। केवल एक मिनट रह गया है। क्या क्वेश्चन कर पाएंगे?

श्री सभापतिः अभी दो मिनट हैं।

श्री नरेश अग्रवालः छोड़िए सर, हम अलग से मंत्री जी के साथ बैठकर डिस्कस कर लेंगे, हमारा और इनका बड़ा गहन रिश्ता है। ...**(व्यवधान)**...

MR. CHAIRMAN: No, no; but there are supplementaries. अगर आपको सवाल का जवाब नहीं सुनना है तो सप्लीमेंटरी सुन लीजिए।

MR. CHAIRMAN: Any other supplementary?

श्री नरेश अग्रवालः श्रीमन्, आपके आदेश पर बहुत मिठास से मैं माननीय मंत्री जी से सिर्फ यह पूछना चाहता हूं कि आपने अपने उत्तर में स्वीकार किया है कि इतने-इतने क्राइम हुए। तो वे कितने परसेंट हैं? आप यह भी मानते हैं कि digital payment अभी टोटल आबादी का 20 परसेंट के ऊपर शायद नहीं हुआ होगा। Digital केन्द्र भी हमारे यहां इतने कम हैं, अगर आप विश्व को आंकें तो चाइना में डिजिटल केन्द्र हमने 6 गुना ज्यादा हैं। अभी डिजिटल केन्द्र भी नहीं हैं। मंत्री जी, सिर्फ इतना बतला दीजिए कि चन्द्रबाबू नायडू जी आंध्र प्रदेश के मुख्य मंत्री रहे हैं, जो इन्होंने अपनी कमेटी की पूरी रिपोर्ट दी है, उस पर उन्होंने यह भी कहा है कि डिजिटल पेमेंट के फ्रॉड जो हों, उसका जो इंश्योरेंस है, वह होना चाहिए और उसकी जिम्मेदारी सरकार की होनी चाहिए, जिससे जिसके साथ फ्रॉड हो, उसको वह रुपया मिलने की गारंटी हो। क्या सरकार उस पर विचार कर रही है?

श्री रवि शंकर प्रसादः सर, insurance की बात सही कही गयी है। भारत में digital payment बहुत बढ़ रहा है और चन्द्रबाबू कमेटी की अनुशंसाओं पर सरकार बहुत गंभीरतापूर्वक विचार कर रही है। बहुत सारी credit card companies इंश्योरेंस देती हैं। हम लोगों की पूरी कोशिश है और मैं नीतिगत रूप से आपके विचारों के साथ हूं। मैं अंतिम एक लाइन कहना चाहता हूं। जितने फ्रॉड हो रहे हैं, हर साल 1,200 करोड़ रुपए के transactions होते हैं, जिसमें एटीएम का फ्रॉड .001 परसेंट है और दूसरा फ्रॉड .007 परसेंट है - यह बहुत ही कम संख्या है, इतना मैं आपको बताना चाहता हूं।

MR. CHAIRMAN: The Question Hour is over. The House stands adjourned till 2.30 p.m.