DAWN

29th November, 2018

Banks issued guidelines to tighten cyber security

KARACHI: In the aftermath of a local bank reporting a loss of Rs2.6 million last month, the State Bank of Pakistan (SBP) on Wednesday issued a number of measures against cyber crime to safeguard banks/microfinance banks (MFBs) and their customers from potential frauds.

Banks and MFBs will immediately carry out extensive vulnerability assessment and penetration testing to identify potential weaknesses in their Alternate Delivery Channels (ADCs) and payment systems including, but not limited to, card systems, RTGS, SWIFT, internet/mobile banking and agent-based/branchless banking etc, said the SBP.

Take a look: 'Almost all' Pakistani banks hacked in security breach, says FIA cybercrime head

"The assessment reports along with action plans and timelines to address the vulnerabilities will be submitted to Payment Systems Department (PSD) latest by March 31, 2019," the bank stated on Wednesday.

In addition to these, banks will also arrange independent third party audit of their ADCs and payment systems. "These reports are to be submitted to PSD latest by Dec 31, 2019," said the SBP.

With effect from Jan 1, 2019, banks/MFBs will send free of cost transaction alerts to their customers through both SMS and email for all international and domestic digital transactions, the SBP continued.

The SBP said banks will be solely responsible for ensuring customer authentication for activation of any ADCs. Further, any loss of customer funds due to false activation of ADCs will have to be compensated by the respective bank/MFB.

"All card-issuing banks will acquire or upgrade the capability to enable their customers to activate or block their cards for online/cross-border transactions as and when required by them, latest by Mar 31, 2019," said SBP.

"These banks will replace all existing payment cards (except social transfer cards) with EMV chip-and-PIN payment cards latest by June 30, 2019," the SBP added.

Banks/MFBs will deploy real-time fraud monitoring tools and alert mechanisms, preferably provided by their payment schemes, to detect potential fraudulent activities on their card systems latest by Jan 31, 2019.

Banks will also make arrangements to monitor on 24/7 basis usage/activity regarding payments made through their cards or online transactions on internet banking platforms. "They will immediately review their existing agreements with payment schemes to identify clauses that may expose them to potential financial, legal and operational risks arising due to cyber-attacks or crimes," said the central bank.

The SBP said the banks will immediately set reasonable per-day transaction limits, commensurate with their risk appetite and transaction volume with the payment schemes especially for cross-border usage. They will ensure that their risk exposure remains within the pre-agreed limits set with the international and domestic payment schemes through legally binding contractual arrangements.

“Banks have been advised to take full coverage of payment schemes’ cyber security threat intelligence,” said the SBP, adding that banks will educate their customers that they will never ask about personal information by phone or email.

In case of knowledge that customer data has been compromised, the banks will immediately protect them from further losses, inform them within 48 hours about the action taken and will compensate the loss within two business days, said the SBP.

Published in Dawn, November 29th, 2018.

Shahid Iqbal