

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

17 JUN 2021

No. 1-5/2003 (NTISB-II)

Islamabad 16 June, 2021

Subject: - Advisory - Safe Use of ATM Cards (Advisory No. 41)

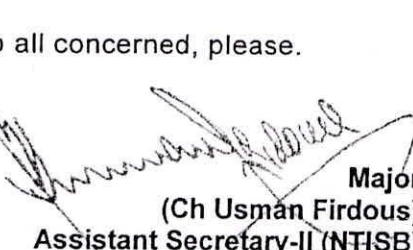
M(Admin/HR)

M(I.T)

A.S(Rev. Div.)

1. Recently, a sharp rise in ATM skimming (ATM fraud) incidents have been reported. Skimmers install Card Reader device on ATM machines to steal ATM card information during a legitimate ATM transaction and subsequently use the stolen information to withdraw cash by duplicating the compromised ATM cards. In such cases, cash withdrawal of account holders who had their ATM cards in their custody were reported from a different city other than their place of residence. This situation warrants cautious use of ATM cards and machines. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned.

2. Forwarded for information and dissemination to all concerned, please.

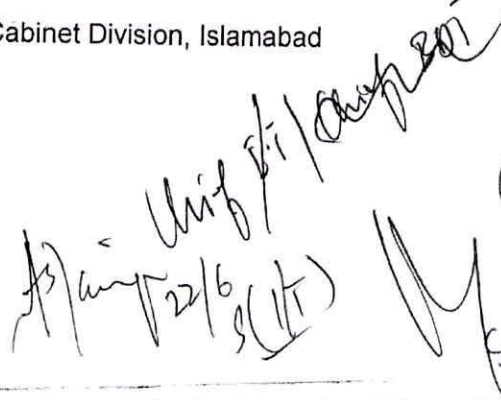

Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

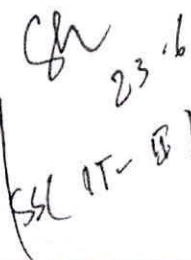
All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Governor, State Bank of Pakistan
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Directorate General, ISI, Islamabad
6. Secretary, NTISB, Cabinet Division, Islamabad
7. Deputy Secretary, NTISB, Cabinet Division, Islamabad
8. Director (IT), Cabinet Division, Islamabad

FBR eCOX Dy.No. 77986-R
Received in Chairman's Sectt.
on 17 JUN 2021


22/6
S(IT)


23.6
SSC IT-B1

Cont'd.....P/2

Subject: - **Advisory - Safe Use of ATM Cards (Advisory No. 41)**

1. **Background.** Recently, a sharp rise in ATM skimming (ATM fraud) activities have been reported. Skimmers install Card Reader device on ATM machines to steal ATM card information during a legitimate ATM transaction and subsequently use the stolen information to withdraw cash by duplicating the compromised ATM cards. In such cases, cash withdrawal of account holders who had their ATM cards in their custody were reported from a different city other than their place of residence. The situation warrants cautious use of ATM cards / machines and safe custody of bank accounts details. Above in view, recommendations at **Para 3** should be followed to prevent becoming victim of such incidents.
2. **Methods to target ATM Machines.** Following techniques may be used by skimmers to withdraw illegal cash from bank accounts: -
 - a. Installing card reading devices on ATM Machines.
 - b. Tiny cameras on ATM machines to get PIN.
 - c. Links sent through SMS / WhatsApp asking for debit / credit card details.
3. **Recommendation**
 - a. Withdraw cash only from ATM machines installed at the bank branch.
 - b. Frequently **change PIN** to avoid PIN compromise.
 - c. **Cover keypad** while typing PIN at ATM machine.
 - d. **Contact concerned bank for alerts** when any activity occur regarding illegal withdrawal against your account.
 - e. **Do not click on malicious or forwarded banking links.**
 - f. Requests for personal or financial information should be avoided and never entertained.
 - g. **Identify spam message;** if it seems urgent, provide some gifts / shocking news or requires to spread it among others.
 - h. Keep personal phones secure and **do not connect to public WiFi** networks.
 - i. In case of any illegal activity pertaining to bank account, inform concerned bank and report the issue immediately to FIA at **helpdesk@nr3c.gov.pk**
4. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk
5. Forwarded for information and dissemination to concerned, please.

* * * * *