Ref. No.: GEN_AWAR/2023-24/005

Date: 25th Oct 2023

To,
The CEO/GM
Head Office

Sub – General Awareness / Dos and Don't's for ATM and ECOM Transactions.

Dear Sir/Madam,

In an age where technology has revolutionized the way we conduct financial transactions, the risk of fraudulent activities has increased significantly. It is our collective responsibility to take proactive steps to safeguard the financial well-being of individuals and institutions alike.

I would like to offer some general Dos and Don'ts on how we can work together to enhance security and minimize the risks associated with ATM and E-commerce transactions:

It's important to follow Below dos and don'ts:

Dos:

1. **Use Secure ATMs:**

    - Use ATMs located in well-lit, secure areas.
    - Prefer ATMs at bank branches or reputable institutions.
    - Check the ATM for any suspicious devices or attachments before using it.

2. **Shield Your PIN:**

    - Always cover the keypad with your hand when entering your PIN.
    - Memorize your PIN; don't write it down or share it with anyone.
    - Avoid using easily guessable PINs like your birthdate.

3. **Protect your card:**

    - Always protect your card by temporary disabling using Card Safe Mobile App.
    - Always set minimum transaction limit by using Card Safe Mobile App.
    - Don't share your ATM card, PIN, or any transaction details with anyone.
    - Be cautious of anyone who offers to help you with your ATM transaction.

4. **Check for Skimming Devices:**

    - Inspect the card slot and PIN pad for any unusual attachments or devices that look out of place.
    - If something looks suspicious or loose, don't use the ATM and report it to the bank immediately.

5. **Monitor Your Account Regularly:**

    - Check your bank statements and transaction history regularly for unauthorized or suspicious transactions.
    - Sign up for transaction alerts from your bank or credit card company.

6. **Report Lost or Stolen Cards Immediately:**

    - If your ATM card is lost or stolen, report it to your bank immediately to prevent unauthorized transactions.
    - Save your bank's customer service number in your phone for quick access.

7. **Use Secure Websites for E-commerce:**

    - Shop on reputable websites with "https://" in the URL and a padlock icon in the address bar.
    - Look for trust seals and customer reviews.

8. **Use Payment Methods with Buyer Protection:**

    - Consider using payment methods like credit cards or services with buyer protection, which can help dispute unauthorized transactions.
    - Avoid using debit cards for online transactions if possible.

9. **Enable Transaction Alerts:**

    - Set up transaction alerts with your bank or card issuer to receive notifications for online and card transactions.

10. **Mobile Lost Reporting:**

    - If the phone suddenly shows SIM card activation error / disconnects from the network, report immediately to the Telecom Operator as this could be a case of SIM cloning / unauthorised duplicate SIM issuance.

Don'ts:

1. **Don't Use Compromised or Suspicious ATMs:**
    - Avoid using ATMs that appear damaged, tampered with, or in poorly lit or isolated areas.
2. **Don't Share Your PIN:**
    - Never share your PIN with anyone, including friends, family, or bank employees.
    - Don't write down your PIN or store it with your card.
3. **Don't Use Obvious or Weak PINs:**
    - Avoid using easily guessable PINs, such as "1234" or "0000."
4. **Don't Let Strangers Assist You at the ATM:**
    - Politely decline offers of help from strangers at the ATM, as they could be attempting to scam you.
5. **Don't Ignore Unusual ATM Behaviour:**
    - If an ATM behaves strangely, retains your card, or fails to dispense money, report the issue to your bank immediately.
6. **Don't Save Payment Information on Untrusted Websites:**
    - Avoid saving your payment information on websites that you don't trust completely.
7. **Don't Click on Suspicious Links:**
    - Be cautious of emails, messages, or pop-ups that ask for your card or personal information. These could be phishing attempts.
8. **Don't Share Card Details Over the Phone:**
    - Never provide your card details over the phone unless you initiated the call to a trusted organization.

By following these dos and don'ts, you can significantly reduce the risk of falling victim to ATM and E-commerce fraud and help keep your financial information secure. Always stay vigilant and use common sense when conducting financial transactions.

Regards,

For Sarvatra Technologies Pvt. Ltd. Pune

Sanjay Sawant

AVP – Customer Support