Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2017-0008

Secure use of Credit/Debit cards

Original Issue Date: January 27, 2017

Description

New technologies have simplified and smoothed business-to-customer experiences with mobile payments, e-wallets, and payment cards. As the online payment processing market grows, user demands for additional payment features and options lead growth in multiple directions. As e-commerce expands, opportunities for fraudulent misuse of payment networks and data theft grow right alongside.

A payment card is a device that enables its owner (the cardholder) to make a payment by electronic funds transfer. The most common types of payment cards are credit cards and debit cards. A payment card is electronically linked to an account or accounts belonging to the cardholder. These accounts may be deposit accounts or loan or credit accounts, and the card is a means of authenticating the cardholder.

A credit card is a payment card issued to users (cardholders) to enable the cardholder to pay a merchant for goods and services, based on the cardholder's promise to the card issuer to pay them for the amounts so paid plus other agreed charges.

A debit card is a payment card that can be used instead of cash when making purchases. It is similar to a credit card, but unlike a credit card, the money comes directly from the user's bank account when performing a transaction.

An ATM card is any card that can be used in automated teller machines (ATMs) for transactions such as deposits, cash withdrawals, obtaining account information, and other types of transactions, often through interbank networks. Cards may be issued solely to access ATMs, and most debit or credit cards may also be used at ATMs.

Best Practices for Users to remain safe

- While making online transactions with credit/debit card, user must only use card at established and reputed sites as there are less chances of card fraud on a reliable website.
- Always ensure that the address of the website where transactions to be done, starts with "https://" and not "http://".
- Always perform online financial transactions from a secure computer system updated with latest security updates/patches, anti-virus and anti-spyware software and personal firewall.
- Change your card PIN (Personal Identification Number) periodically
- Do not disclose any personal information online like your date of birth, billing address, etc., on the Internet because that can be misused in order to unlock your account password.
- Never share card details over the phone or with anyone in person as it is easier way for others to get access to your credit card confidential information and make the online transactions.
- Do not send card and account details through e-mail to prevent from malicious use by others
- Regularly check account statement related to the card and notify the card company in case of any discrepancy.
- Ensure whether your card is enabled/disabled for International use, disable if it not necessary. Check with your bank for any additional options such as restricting the usage of cards on different payment channels viz., PoS/ATM/E-Commerce or Domestic/International usage time-to time through bank's own interface/app.
- Never leave your card unattended
- Keep card help line phone numbers with you for any kind of assistance

References

CERT-In
CIAD-2016-0068: Securing online Banking
CIAD-2016-0083: Personal online security

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India