MAHARASHTRA CYBER

2025

DIGITAL CARDS
Real Threats

ADVISORY REPORT

CCCMH_CA_2025_04

Carding fraud is rising in India—your card details can be stolen and misused in seconds. This advisory explains how it happens, recent trends, and how you can stay safe.

Stay Alert! Swipe Smart.

TABLE OF CONTENT

EXECUTIVE SUMMARY

Carding fraud is a form of cybercrime where criminals use stolen debit or credit card details to make unauthorized transactions. With **India's surge in digital payments, especially via UPI and cards, these crimes have grown rapidly.**

Key Takeaways:

1. **Rapid Growth:** Over 12,000 credit card fraud cases reported between April–Sept 2023, involving ₹630 crore.
2. **Stolen Data Sold Online:** Card information is traded on the dark web and used globally.
3. **Common Attack Vectors:** Phishing, skimming, fake payment portals, and malware.
4. **Widespread Impact:** Victims face financial loss, emotional stress, and trust issues.
5. **Awareness Saves:** Timely detection, strong digital habits, and prompt reporting are critical.

RISING CARDING THREATS IN INDIA

With increasing **mobile and internet penetration**, India's **large digital population** has become a **prime target for global fraud networks.** Carding is no longer limited to international players; **local syndicates are now actively involved,** targeting **small-town users** and **first-time digital adopters. Empowering citizens with information and preventive strategies** is critical to **reducing exposure** and **building trust in the digital economy.**

INTRODUCTION

UNDERSTANDING CARDING FRAUDS IN INDIA

India's shift to a digital economy has enabled quick and convenient financial transactions but also opened the door to cyber threats. **Carding frauds** is one such threat where fraudsters use stolen card credentials to perform illegal transactions. These credentials are often harvested through **phishing, ATM skimming, or online data breaches.** Once obtained, criminals use the card details to make unauthorized purchases or transfer funds, often before the victim even notices.

THE HIDDEN DANGERS OF CARDING FRAUD

This advisory aims to educate citizens about the **risks of carding fraud** and provide **preventive strategies** to mitigate the impact of such cybercrimes. As digital payments continue to rise across India, it's crucial for individuals to recognize the signs of fraud and adopt safer online practices. **Awareness and vigilance** are key in safeguarding personal and financial information.

WHY CARDING FRAUD IS HARD TO DETECT

What makes **carding fraud** particularly dangerous is its **stealth and scalability.** Victims often don't realize their data has been compromised until their funds are gone. Fraudsters target the **most vulnerable**, especially **first-time digital users** and those from **smaller towns.** The **anonymity of digital platforms and cryptocurrencies** makes it even harder to trace and prosecute them.

THE EVOLUTION OF CYBERCRIME AND ITS IMPACT

The **rise of carding frauds** signals a shift in criminal tactics—from **physical theft** to **digital exploitation.** Fraudsters now use **online loopholes, social engineering,** and the **dark web** to steal funds discreetly. As **digital reliance grows, public awareness** and **strong digital hygiene** are essential. Citizens must **stay alert** and **report suspicious activity** to reduce losses and prevent further fraud.

THREAT LANDSCAPE

Carding frauds in India have become increasingly sophisticated, with criminals leveraging a **mix of social engineering, malware,** and **underground marketplaces** to carry out financial crimes. Understanding how carding works and the tools fraudsters use is key to protecting oneself.

Carding networks in India are now **highly organized,** using **automated bots, malware,** and **underground markets** to trade and test **stolen card data.** The rise of **instant and contactless payments** has made fraud **faster and harder to detect,** leaving users **increasingly vulnerable.**

HOW CARDING WORKS?

Carding is a **multi-step process** that **starts with the theft of credit or debit card details** and **ends with unauthorized transactions or digital laundering.** Here's how it typically unfolds:

HARVESTING CARD DETAILS

Cybercriminals steal sensitive card details—like number, name, expiry, and CVV—using illicit methods, then sell them on darknet markets, often priced by bank, card limit, or location. These stolen credentials are later used for unauthorized online purchases or financial fraud.

CARD TESTING

To verify that a card is still active and usable, fraudsters conduct small-scale transactions—usually on low-risk e-commerce platforms. These are often for minor purchases like online subscriptions, digital tokens, or games, which don't raise red flags.

EXPLOITATION

Once verified, the card is used for high-value purchases or digital goods like gift cards or crypto, which are then resold for cash. Stolen funds are often laundered via mule accounts or online platforms to hide the trail.

NOTE: This entire process is often automated using tools like BIN checkers, carding bots, and VPNs/proxies to hide identity and bypass location-based security mechanisms.

TACTICS EMPLOYED

by Carders

Carding attacks can occur through multiple vectors. The most common tactics in India include:

PHISHING

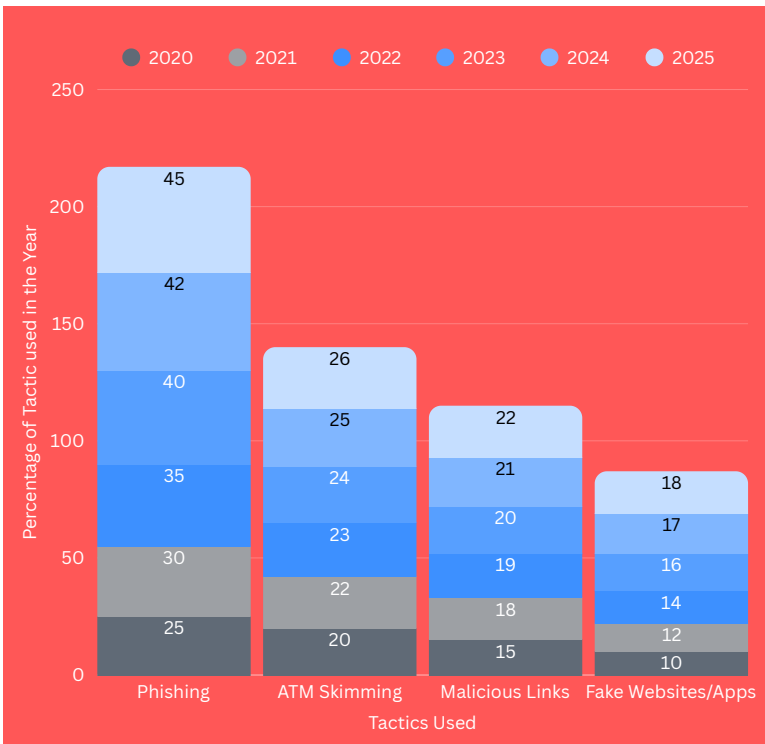
Fraudsters send **fake emails, SMS (smishing),** or make **calls (vishing)** pretending to be from **banks** or **government bodies (like RBI or police)** to trick users into revealing their card details. These messages often create a **sense of urgency**—such as **fake warnings** about account suspension or rewards for updating KYC information.

ATM SKIMMING

Small, discreet devices are illegally attached to **ATMs** or **point-of-sale (POS) terminals** to "skim" card information during legitimate transactions. Hidden cameras may also be installed to capture **PIN codes.** These details are then **cloned** onto blank cards and used for **withdrawals** or **purchases.**

MALICIOUS LINKS AND FAKE WEBSITES

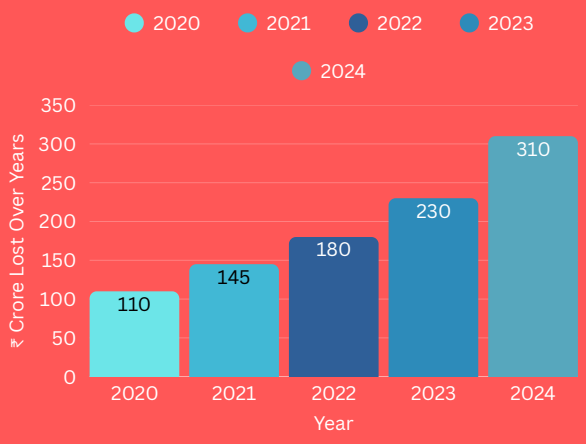
Fraudsters create **fake banking portals, UPI apps,** or **shopping websites** that look identical to legitimate ones. Unsuspecting users who input their **card data** on these platforms unknowingly hand over their information to **criminals.** Often, these links are spread via **WhatsApp forwards, pop-up ads, or fraudulent apps.**



RECENT INCIDENTS

India's rapid adoption of **digital transactions has positioned it as a global leader in digital payments.** However, this growth has also led to a significant increase in digital financial crimes, including carding frauds. In **fiscal year 2024,** high-value cyber fraud cases in India surged over fourfold compared to the previous year, resulting in **losses of approximately $20 million.**

The rise in such frauds is attributed to factors like **low cyber literacy, widespread data exposure,** and the use of **sophisticated technologies** by scammers. Notably, incidents like the **Valmiki Corporation scam** in Karnataka, where **₹94 crore intended for tribal development** were misappropriated, highlight the severity of the issue.



GUJARAT BANKING FRAUD SURGE (FY2024)

In **FY2024,** Gujarat experienced a **469% increase in digital banking frauds,** with losses amounting to **₹49.92 crore.** Common fraud methods included sharing of **ATM, debit,** and **credit card PINs** and **CVVs** over the **phone**, as well as clicking on dubious links received via **WhatsApp** and **SMS.**

NOIDA FAKE CREDIT CARD GANG BUSTED (DECEMBER 2024)

In **December 2024, Noida Police** arrested **six individuals** involved in a sophisticated **credit card fraud scheme.** The gang targeted credit card holders by promising to increase their card limits through **fake websites** resembling authentic bank portals. They collected **sensitive information** and made unauthorized purchases on online platforms like **Flipkart.**

BHOPAL CREDIT CARD SCAM (MAY 2024)

In **May 2024,** the Cyber Crime unit of the **Bhopal Police** arrested **four individuals from Delhi** for allegedly **duping people by posing as bank employees.** They offered **free credit cards** and **easy loans, sending fake website links** to collect personal information. One victim reported a **loss of over ₹60,000** after providing details on a fraudulent **ICICI Bank credit card** link.

RECOMMENDATIONS

FOR CITIZENS

- **Guard Your Card:** Never share card details and avoid suspicious links or apps.
- **Track Every Transaction:** Activate SMS/email alerts and review statements regularly.
- **Practice Digital Safety:** Use **strong passwords**, update apps, and enable **two-factor authentication.**

FOR VENDORS
(Shopkeepers, E-Commerce Platforms)

- **Secure Payment Channels:** Use **trusted POS machines** and certified **online gateways.**
- **Verify High-Risk Transactions:** Manually check suspicious or unusually large purchases.
- **Raise Customer Awareness:** Display notices about safe card usage and caution against phishing.

FOR BANK/CARD PROVIDERS

- **Invest in Smart Security:** Use AI-driven fraud detection and dynamic authentication.
- **Promote Safer Cards:** Roll out tokenized and virtual card options for safer online use.
- **Support Victims Quickly:** Improve dispute redressal systems and conduct awareness drives.
- **Enhance Collaboration:** Work closely with law enforcement and cybersecurity agencies to trace fraudsters.
- **Continuous Customer Education:** Regularly send educational messages, app alerts, and organize webinars on digital safety.

REFERENCES

THE TIMES OF INDIA

https://timesofindia.indiatimes.com/city/ahmedabad/banking-fraud-in-gujarat-sees-a-469-increase-in-fy24/articleshow/111999152.cms?utm_source=chatgpt.com

INDIA TV

https://www.indiatvnews.com/uttar-pradesh/noida-police-bust-fraud-credit-card-gang-six-accused-arrested-video-2024-12-14-966241?utm_source=chatgpt.com

THE NEW INDIA EXPRESS

https://www.newindianexpress.com/cities/delhi/2024/Dec/04/delhi-police-crackdown-on-cyber-fraud-racket?utm_source=chatgpt.com

INDIA TODAY

https://www.indiatoday.in/cities/bhopal/story/bhopal-police-arrest-4-for-duping-people-with-credit-card-loan-offers-2541218-2024-05-20?utm_source=chatgpt.com

PROTECT YOUR CARD,
PROTECT YOUR MONEY

Call 1945

mhcyber.gov.in