Zee Business (Hindi)

A new game of online fraud! Don't make these 10 mistakes, your entire account could be empty in a flash.

Date: 15/11/2025| Edition: Online | Page: NA | Source: Kumar Surya

---

Digital payment safety tips: The trend of digital payments has grown so rapidly across the country that now everything from everyday purchases to large electronic items is being done through online transactions. Whether it's UPI, credit cards, or wallet payments, people are now trusting digital more than cash. But where there is convenience, there is also danger. Risks such as online payments, fake offers, screen-sharing fraud, and phishing are constantly increasing. In view of this, SBI Card has issued very important warnings for customers.

Shop only on trusted websites

Today, thousands of links circulate on social media and messaging apps, many of which are fake. Customers should always shop from a brand's official website or a trusted e-commerce platform. Clicking on random links is the easiest route to digital fraud.

Beware of screen sharing fraud

Many users are lured by strangers and share their screens. No app, no agent, no bank ever asks you to share your screen. Downloading any third-party app (such as an unknown APK file) is a direct invitation to fraud.

The trap of Dream Deal

These days, fake websites lure customers by offering discounts of up to 70%, 80%, or even 90%. Verify such offers with the brand first. If an offer seems “too good to be true,” it's almost certain to be fraudulent.

Most frauds related to Reward Points

Credit card users often receive SMS messages saying, "Your reward points are expiring. Redeem immediately." Such messages are a common fraud. Do not click on any links or share your OTP, card number, or CVV with the caller.

Turn on alerts for every transaction

If an unauthorized card payment is made, SMS/app notifications will alert you immediately. Therefore, all users should ensure that SMS and in-app alerts are enabled. This can prevent fraud within minutes.

Phishing calls and emails

Fake emails and calls say things like, "Your account will be blocked..." "Your points are expiring..." "Your KYC is incomplete..." Always verify any such information with official customer service. The bank never asks for an OTP, PIN, CVV, or password.

Keep your mobile and apps updated

Cybercriminals primarily target older phones, outdated browsers, and outdated apps. Always keep your phone, browser, and payment apps updated. This increases your protection against malware and viruses. Also, always turn on multi-factor authentication.

Keep strong passwords

Passwords for email, banking, and social media should not be the same. Change them frequently.

Never share card information

Many people post their card number, mobile number, or screenshots on Twitter or Facebook when filing a complaint. This is extremely dangerous. No bank ever asks for such information on social media.

Fake refund blast

If you receive an SMS saying, "Your account has received a refund. Please claim it," first check your balance in your bank app. Don't open any links without verifying.