# Check portal's credentials and opt for safer options to avoid mistakes when e-shopping

E-retailers are wooing customers with unbelievable discounts across categories. While online shopping offers obvious advantages such as convenience, ease of comparison, home delivery, refunds and, most importantly, lower prices, it also entails certain risks. When you pay online by using your credit or debit card, you expose yourself to the possibility of fraud. Here are five mistakes to avoid when you shop online this festive season.

**Shopping on Unsecure Portals**

A lot of establishments now sell online, but you need to identify the credible ones to make sure that your data is secure. Do not shop on obscure websites promising fabulous discounts. "Dualfactor authentication and the one-time password mechanism have helped increase customer confidence. However, customers need to exercise due diligence while shopping to ensure secure transactions," says Anil Ramachandran, executive vice-president and head, retail unsecured assets, credit cards and personal loans, IndusInd BankBSE 0.70 %. Make it a point to type out the URL of the shopping portal instead of clicking on links that pop up on search engines.

"While conducting online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or an 'https' URL — where the 's' stands for 'secure' — rather than 'http'," says Abonty Banerjee, general manager and head, digital channels, ICICI BankBSE 2.11 %. One simple way to reduce the risk of fraud is to use the virtual card facility that many banks offer. You can create the 'card' by transferring funds from your account. Since the balance on this card and its validity are limited, you can shop without exposing your bank account to risk.

**Using Public Computers & Networks**

It may be tempting to use free, open Wi-Fi to shop, but this can be risky. "Never use public computers or public Wi-Fi connections to make any financial transactions such as payments," says Jairam Sridharan, president, retail lending and payments, Axis BankBSE 3.97 %. Unsecure connections or malware installed in such machines could result in your data being stolen. If you must use a public computer to carry out a transaction, change your password as soon as possible when you reach home or office.

**Prey to Phishing**

Despite repeated warnings by the Reserve Bank of India (RBI) as well as banks, many customers remain unaware of the consequences of parting with credit card and bank account details. Fraudsters are able to obtain the information from unsuspecting victims and then use it to siphon funds from their accounts. Do not forget these basics in the hurry to click the link in your e-mail offering a 'never-before-seen' discount on the latest gadget or smartphone, in return for your

account details and credit card information. "Be cautious of mails, calls, SMSes that come from unrecognised senders and ask you to confirm personal and financial details. Do not disclose details like passwords, card numbers, expiry details, CVV and the 3D Secure Pin to anyone, even if they claim to be bank employees or from government establishments," says Banerjee.

**Not Registering for Mobile Banking**

If a fraud has been committed, how soon you get to know of it becomes critical. Mobile alerts are helpful as the customer is immediately informed about the use. If you register yourself for mobile banking at the time of opening the bank account or later, your bank will send you an alert for every transaction. The moment you realise that an unauthorised transaction has taken place, you can alert your bank and get it blocked. If you are able to inform it in time, your bank will compensate you for any loss. The onus of proving that the fraud took place due to the customer's negligence is now on the banks. Apart from this, since banks and card issuers send onetime passwords to your mobile while completing payments, your transactions will get an additional layer of security.

**Not Checking Statements Regularly**

It is a good practice to go through your account and credit card statements. If you spot a suspicious entry, report the matter to the bank immediately. Also, make it a point to save your bank's customer centre numbers in your cell phone as well as mailbox. Contact details are also printed on the back of credit and debit cards. If your bank fails to resolve your complaint, you can escalate the matter to the nodal officer and subsequently to the banking ombudsman.

*(Economic Times)*