What Are Different Types of Credit Card Fraud

You are wrong if you think hacking is the only way of scamming an individual! There are many ways one can get trapped in fraudulent activities. Here are some of the examples;

1. Skimming

In this type of scam, your credit card details are stolen with the help of a device called a skimmer. When your card gets swiped through a skimmer, it stores all the data from your card. This information can then be duplicated on another card.

Thus, scammers use your credit card information to make monetary transactions. So, the next time you use credit cards, ensure you do not swipe through any machine that looks suspicious. You can also use chip-based credit cards; these are much more secure than those with a magnetic strip.

2. Dumpster Diving

Quite often, people casually discard bills or documents which contain their credit card details. Anyone can collect them to retrieve their bank details and use them for scamming. This process is known as dumpster diving.

Hackers can use such documents with sensitive information for malpractices. Therefore, the next time you have any such documents to discard, either shred them or scratch those details. Following certain precautionary steps can prevent you from getting trapped in such types of credit card scams in India.

3. Phishing

Phishing involves persuasion. Suppose you receive an email that looks convincing as it is from a well-known bank or financial organisation. Your general reaction would be to click and check what it is about. Once you click on the link, it will redirect to a strange website where you are asked to put your personal information.

Most people fall into these traps. You must always remember banks do not generally send emails requesting your details. If you ever receive any such email or SMS, make sure to inform your credit card issuer so that you do not get into the trap. In addition, you must be very observant while replying to any such email or SMS.

4. Keystroke Capturing

Hackers mostly use keystroke logging through certain software to find your credit card details. This can happen if you click on a link redirecting you to download malware, and you unknowingly do that. If any such software gets installed in your

system, it will record every key that you press. Hence your ids and passwords are recorded as well.

To avoid any such situation, make sure not to click on any suspicious links. You can also use a virtual keyboard while feeding personal information like passwords and id details. Lastly, you must have reliable antivirus software to protect your system.

5. SIM Swap

Cybercriminals can call any mobile operator and pretend to be a credit card holder requesting a duplicate SIM card. In addition, they would ask the operator to deactivate the original cardholder's number. So, now the scammer can create new IDs, receive OTPs and execute online transactions.

If you ever receive a warning regarding a duplicate sim request or feel your number has been blocked. Immediately inform your mobile service operator and report about this. If you remain cautious and let the service provider know at the time, you will be able to prevent such scams.

6. Application Fraud

When identity theft happens, someone tries to impersonate you by using stolen documents to get a credit card under your name. If any criminal successfully completes this task, he will have a valid card to perform all kinds of monetary scams.

To avoid this kind of situation, you must keep track of whenever your IDs and other documents are used. In addition, if you have multiple copies of the same document and want to discard them, shred them before dumping them.

7. Hacking

One of the most common types of credit card fraud in India must be hacking. It is probably the oldest method of performing fraudulent activities. With the advancement of technology, hackers are also developing their skills. They can hack any of your devices and steal all your personal information.

Similarly, hackers can steal data from those firms with whom you have performed transactions. Thus, they can breach data for scams.

Although it is unpredictable to notice when you are hacked, so you need to be very careful while performing online transactions. If any website seems suspicious, do not provide your details. You also must not click on every link you get. These hackers can break into your online space and get the required data for conducting scams.

What Are the Ways to Avoid Credit Card Fraud

There is nothing to be afraid of. Here are some of the tips that you should follow to steer clear of credit card fraud.

1. Keep Your Card Safe

The primary step is to keep your card in a safe place so that it is not easily accessible to others. After swiping your credit card, always check if the magnetic strip or back of the card is hampered in any way.

2. Monitor Online Transaction

Most banks send an alert SMS after every online transaction. Another way of tracking your transactions is by installing your bank's app. It helps you check your account balance and other details whenever needed.

3. Review Billing Statements

To prevent different types of credit card fraud, one basic thing you should do is review your billing statements. This will allow you to note if any unknown or unauthorised transaction has been reported.

4. Avoid Paper Trials

Another easy step that can prevent credit card scams is by shredding your billing statements. Credit card statements generally contain the full credit card number, so when you want to discard them, ensure shredding the document.

5. Signing Blank Receipts

While signing credit card receipts, ensure the amount is verified. If you notice any blank spaces, make sure to cross-check with your bank regarding this.

6. Never Make It Public

Your credit card details are very sensitive, so always beware of phishing. You must never share your card number, CVV or PIN through any text messages. Keep it memorised and also keep changing it after an interval.

7. Always Double-check

Scammers can mimic a bank or business' logo that requires personal information. So, it is better to always double-check the website or merchant prior to purchasing. If you feel there is any discrepancy, do not complete your payment details.

8. Report Lost/ Stolen Card

Suppose your wallet was lost or stolen, and it contained your credit card. Your first step in regard to this is to report and block your card as soon as possible. You must always keep the customer service number of your credit card company in your contacts so that you can immediately report the incident.

9. Create Strong PINs and Passwords

Avoid using a birthdate, anniversary date, or contact number as your credit card PIN or password. As most website suggests, you must combine the following to create a responsible password -

- Upper case characters
- Lower case characters
- A special character
- A numerical digit

10. Using RFID-blocking Wallets

Contactless cards are embedded with an RFID chip that allows smoother transactions. However, any fraudster can scan the RFID data while standing beside you. This is why it is recommended to invest in an RFID blocking wallet so that your cards become more difficult for scammers.