Cyber frauds: How to avoid losing money to fraudsters

The chances of recovering lost money due to cyber fraud are low. Take precautions instead, like avoiding clicking on links shared on SMSs and emails without first verifying the sender's authenticity.

MAULIK M | JANUARY 04, 2024 / 10:18 AM IST

A bank never asks a customer to share sensitive information, such as a bank account number, credit card number, CVV, OTP, or

RELATED STORIES

Chartered accountants may soon have to file tax returns for robots: Experts

Will mis-selling of insurance stop after consumer affairs ministry's proposal? Unlikely, say exper...

The Magnificent Seven is not the only concentration America should worry about

To ensure it has up-to-date information on customers, a bank needs to periodically update the personal information in its records or do what is called a re-KYC (**know your customer**). Now, while a bank may inform you about the need for a re-KYC via an SMS, it will never ask you to do the re-KYC by clicking on a link sent on an SMS.

Such SMSs typically come with a fake warning – your account will be blocked within the next 24 hours – forcing you to act in haste.

"If you click on the link, you are led to a page where you have to fill in your details, and the **fraudster** gets all the information he needs to access your bank account. Then, once you share the OTP you have received, he can transfer money out of your bank account," explains Sachin Dedhia, Founder of Skynet Secure Solutions, a company specialising in cyber security and digital forensics.

It helps to remember that a bank never asks a customer to share sensitive information, such as a bank account number, credit card number, CVV, OTP, or password with them.

Shrikrishna Dikshit, Partner – Cyber Security, Nangia & Co LLP, talks about how banks are sending alerts to their customers on how not to fall for scams. But people need to read about these things, become more aware, and stay vigilant.

HOW TO DODGE CYBER FRAUDS

✗ Never click on links in SMS or email allegedly sent by banks	✓ Likely to be fraud attempt. Contact bank branch / helpline /use online banking to check if any action needed from you
✗ Don't download email attachments unless from known sources	
✗ Never share OTPs, passwords, bank account / card numbers	
✗ Don't keep big balance in bank accounts used for transactions	✓ Set transaction limits for bank / card transactions. Can be set via online banking.
✗ Never click on QR codes allegedly sent for refunding money	✓ QR codes are needed for payments not for receiving money. Click on them only if from trusted sources.
✗ Don't google search for helpline numbers. Can be fake.	✓ Search for them on bank / hotel /service provider's website
✗ When installing mobile apps, don't allow access to contacts, photos etc. If app disallows it, best not to install.	✓ Install mobile apps of trusted entities only. Watch out for fake apps with names similar to genuine apps.
✗ Don't store any (or at least critical) data on mobile phones	✓ Subscribe to iCloud or Google Drive to store data / info
✗ Avoid using public wi-fi at airports, malls etc. for transactions	✓ If you must, then use it only for browsing or emailing
✗ Don't install free computer softwares. Can contain malware that steals your data.	✓ Download only licensed softwares from trusted sources
✗ Don't use old versions of banking and merchant apps	✓ Install the latest launched apps that have upgraded safety features

Source: Based on inputs from Shrikrishna Dikshit (Nangia & Co LLP) and Venkat Narayanan (Worldline)