HDFC BANK

SECURE BANKING

NEVER SHARE

OTP • Card Number • UPI PIN • Bank Details • Customer ID & Password

PHISHING & SMISHING LINKS

Frauds

- Fraudsters create third party websites to transmit link via SMS, Email, Social Media Posts, Instant Messenger, etc.
- When you click on the link, you'll be taken to a phishing website that seems extremely real, and you'll be prompted to enter your bank information.
- Once you finish the process, a fraudster will exploit your details to perpetrate the crime.

Security Tips

- The first line of safety against phishing is to know that your bank will never ask for your credentials or send you links to their website.
- Block your card or change your password immediately to avoid the risk.

VISHING CALLS

Frauds

- You may be contacted by a fraudster posing as a banker, firm executive, or insurance agent using information obtained online.
- They can press it as an urgent matter and gain your trust by knowing basic facts about your bank and branch to seek credentials.
- Once the imposter gains your trust, they will ask you to update your KYC, offer you attractive discounts, request a payment to avoid penalties, and so on, all to defraud you.

Security Tips

- Block your card immediately.
- Reset your password frequently.

HDFC BANK | SECURE BANKING | INTERNATIONAL FRAUD AWARENESS WEEK November 14th - 21st 2021 | MOOH BAND RAKHO

FRAUD USING ONLINE SELLING PLATFORMS

Frauds

- Fraudsters pose as buyers on online selling platforms and express interest in your product.
- Instead of paying money, they 'request money' through UPI apps and insist you to approve it to withdraw funds from your account

Security Tips

- Immediately Report unauthorized transaction incidents to your Financial Institution.
- Contact National Cyber Crime Helpline number 155260 to file your complaint.

FAKE HELPLINE & SCREEN SHARING APP TO STEAL CREDENTIALS

Frauds

- Customers use search engines to look up for helpline numbers of businesses, where the scammer has uploaded bogus numbers in order to encourage the customer to call.
- The fraudster pretends to represent the bank and gains access to your device by asking you to download apps and share your screen or ask for your card details for verification.
- Assuming they're genuine, we compromise our secure details.
- Through which they gain access to your banking credentials and later withdraw money using payment apps or internet banking.

Security Tips

- Never download apps and share your screen with an unknown person.
- Always visit your branch if you're facing an issue.

HDFC BANK | SECURE BANKING | INTERNATIONAL FRAUD AWARENESS WEEK November 14th - 21st 2021 | MOOH BAND RAKHO

IMPERSONATING THROUGH SOCIAL MEDIA

Frauds

- Fraudsters set up phony accounts on popular social media platforms and ask for money to pay medical bills or payments.
- They gain your trust over time and use private information later to blackmail and extort money.

Security Tips

- Always verify genuineness of an online account and get suspicious if they ask about confidential information.
- Contact National Cyber Crime Helpline number 155260 to file your complaint.

LOTTERY FRAUD

Frauds

- Fraudsters may write you an email or call you, claiming that you have won a huge lottery prize. However, to receive the funds, it is necessary to verify identity by bank account or credit card on their website, where data is collected.
- In certain circumstances, the fraudsters demand upfront payment of taxes, shipping fees, processing fees, and other fees to get the lottery / goods.
- Because the requested money is a very small percentage of the lottery/goods, the victim may fall prey to the fraudster and make payment.

Security Tips

- Never respond to lottery winning related calls/SMS/Emails
- Notify your bank or credit card issuer to avoid inconvenience

FAKE ADVERTISEMENTS FOR EXTENDING LOAN BY FRAUDSTERS

Frauds

- Fraudsters create phony advertisements for personal loans with very attractive interest rates, easy repayment options, and so on, and then ask customers to contact them.
- These email ids will be look-alike emails IDs of senior bank executives in order to build credibility with naive customers and instil confidence.
- When consumers approach fraudsters for loans, they demand different upfront fees such as processing fees, GST, interstate costs, and so on, and then disappear without disbursing the money.

Security Tips

- Avoid investing in the conversation and contact your relationship manager to avail loans
- Be cautious and ask multiple questions only they would know the answer to.

ONLINE JOB FRAUD

Frauds

- Fake job search portals are developed, and the account is compromised when the victim provides secure bank account, credit card, or debit card credentials on these websites for registration.
- In some circumstances, the con artists impersonate authorities from a reputable corporation and confirm selection after conducting phony interviews. The victim is pressured into paying for a mandatory training program.

Security Tips

- Always use verified job portals.
- Do not respond to generic emails from an unknown company as it could be a scam.

HDFC BANK | SECURE BANKING | INTERNATIONAL FRAUD AWARENESS WEEK November 14th - 21st 2021 | MOOH BAND RAKHO

ATM CARD SKIMMING

Frauds

- Skimming devices have been found in ATM machines, allowing fraudsters to take data from your card and capture your PIN via Installing a dummy keypad and a small / pinhole camera that is effectively hidden from view.
- Other times, fraudsters may pose as other customers nearby and acquire access to your PIN while you are entering it. This information is then utilized to make a duplicate card and take money from the customer's account.

Security Tips

- Check if there's any tampering done to the ATM.
- Always keep an eye for suspicious people around you.

SIM SWAP

Frauds

- Because your registered mobile number is linked to most of your account information and authentication, fraudsters attempt to acquire access to your SIM card or obtain a replica SIM card to carry out digital transactions using the OTP received on the duplicate SIM.
- Fraudsters usually call customers pretending to be from a network company, demanding information in exchange for a free upgrade from 3G to 4G or a bonus on the SIM card.

Security Tips

- Get suspicious if you don't have mobile network in your phone for considerable time
- Contact Mobile operator to ensure that no duplicate SIM is being issued for your SIM.

HDFC BANK | SECURE BANKING | INTERNATIONAL FRAUD AWARENESS WEEK November 14th - 21st 2021 | MOOH BAND RAKHO

FRAUDULENT LOANS WITH FORGED DOCUMENTS

Frauds

- These frauds occur when a person or an entity uses forged documents for availing any form of services from financial institutions.
- Such frauds can happen while sharing the KYC related documents with entities without verifying the authenticity of the NBFC employee / NBFC's email id.
- Fraud loans are also sanctioned on basis of identity thefts by stealing personal information of the victims such as identity cards, bank account details, etc. and using this information for availing benefits from a financial institution.

Security Tips

- Always verify the authenticity of the NBFC employee/company before sharing your credentials.
- Secure your identity cards, bank account details, etc. to avoid identity theft.

COMPROMISE OF AADHAR OTP

Frauds

- Digital accounts can be opened with Aadhaar based OTP.
- There have been instances wherein customers share their UIDAI OTP to 3rd party vendors, hence helping fraudsters in creation of mule accounts.

Security Tips

- Do not share your Aadhaar OTP with unverified institutions.
- Always verify the identity of the person before sharing any information.

HDFC BANK | SECURE BANKING | INTERNATIONAL FRAUD AWARENESS WEEK November 14th - 21st 2021 | MOOH BAND RAKHO

HDFC BANK

INDIA'S No.1* BANK

SECURE BANKING

For more details,
visit HDFC Bank's Secure Banking Page
https://www.hdfcbank.com/personal/useful-links/security

*Based on Retail Loan book size (excluding mortgages).
Source: Annual Reports FY 19-20 and No.1 on market capitalisation based on BSE data as on 31st Dec, 2020