बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
एक परिवार एक बैंक
प्रधान कार्यालय : 'लोकमंगल', 1501, शिवाजीनगर, पुणे - 411005.
H. O.: 'Lokmangal', 1501, Shivajinagar, Pune - 411005.

Beware of frauds through fake Investment/Part time Job/Ponzi Schemes

It has been noticed that Cyber criminals are targeting potential victims by way of offering fake Investment schemes, Part time jobs and Ponzi schemes etc.

In this modus operandi:

- Victims are lured through 'Part time job offers', 'Earn Online' and other investment schemes on internet/social media and/or messaging platforms etc., and are promised high commissions/returns such as doubling of money or usually unrealistic return in short span of time.
- Majority of websites used by fraudster have domains – 'xyz' and 'wixsite'. Most of these sites either redirect to a messaging platform or to a website which has embedded messaging platform link which, on clicking, again redirects to a chat.
- Fraudster pretend to be buyers on online sales platforms and show an interest in seller's products, instead of paying money to the seller, they use to 'request money' option through the UPI app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.
- Fraudster contact customers via emails, social media, etc. and convince them to receive money into their bank accounts (Money Mule), in exchange for attractive commissions, the money mule is then directed to transfer the money to another money mule's accounts, starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- Lottery frauds Fraudsters send emails or make phone calls that a customer has won a huge lottery. However, in order to receive the money, fraudster ask the customers, to confirm their identity by entering their bank account/ credit card details on a website from which data is captured by the fraudsters & ask the customers to pay taxes/forex charges/upfront or pay shipping charges, processing/handling fee etc., to receive the lottery/product.
- Fraudsters approach the customers through telephone call/social media posing as bankers'/company executives/insurance agents/govt. officials, etc. & ask for OTP/ login credentials and other banking security information in return for some money or getting some offers.

We request your attention on below mentioned precautions in order to protect your card/account from such frauds:

- Do not share OTP, login credentials such as CVV number, password etc. with anyone for lucrative offer & investment, you may receive call, SMS, E-mail or Social Media etc.
- Do not send money as initial Deposit, commission or transfer money to anyone claiming to provide doubling of money or unrealistic returns from unknown source.
- Do not respond to the advertisement for Part-time job offers, Earn Online, Ponzi schemes, Investment on Internet, Social Media and /or messaging platforms etc. and which are promised high commissions, returns, doubling of money in short span of time.
- Do not respond to unknown link, email, majority of website used by fraudster have domains-xyz and wixsite.
- Do not share OTP, card number, CVV number, password over phone/social media claiming to be Bank officials, Bank officials never ask for **OTP, PASSWORD** etc.
- Do not respond to calls where the caller asks you to download screen sharing apps.
- Beware of fake customer care numbers that you may find on search engine, before calling always verify the authenticity of such number through their official's website, please also note that customer care numbers are never in the form of mobile numbers.
- Do not allow others to use your account to receive or transfer money for fee/commission.

One Family One Bank
Team Bank of Maharashtra