DIGITAL FRAUD ALERT
MAINTAIN SECRECY & DISCARD GREED

While digital services make banking and other financial services more accessible, it also opens up the system to hackers and fraudsters who commit cybercrimes. They take advantage of the low awareness among users and some loopholes, particularly among the elderly and new users. Incidents of fraud have increased in the past few days, during the lockdown. Remember the golden principle of not sharing any personal information, account number, password, OTP and PIN with anyone, in any form. Always remember that no bank, insurance company, SEBI, RBI, NSDL, stock exchange or government department will ever call you or email you asking for any such information. Only a fraudster will try do so.

Phishing emails asking for Donations to the PM/CM Relief Fund:

These scams feature requests for donations to help with 'medical preparations and supplies' to help the government cope with coronavirus.

'Track the Virus' Technology Scams:

These sorts of phishing attempts have been sent out via both email and text. They encourage people to download software/apps that can help track the spread of the virus. The download infects the computer or phone with ransomware and demands payment to restore the device. We encourage users to download and use Aarogya Setu App for COVID-19 related authentic information.

E-mails Impersonating WHO or Indian Government:

If you get an email claiming to be from one of these top-level organisations, a red flag should trigger in your mind immediately. This email asks people to provide their bank account details so a 'payment' from the help scheme can be deposited. Payment will happen, but not to your account, rather out of your account to a fraudster.

Warning Signs of a Phishing Campaign

Time pressure to Act:
To make victims skip over details they would
usually notice, phishing emails often have a sense of urgency about them. Look out for instructions such as 'Alert From MoHFW or 'URGENT: From INGOV'.

Suspicious Links:
Many phishing emails will ask you to click on a link. Before you click on any link in any email you should always hover over the link with your cursor before taking further action. If the link itself does not match the one in the email, it's likely to be a phishing scam.

Spelling or Grammatical Errors:
Good business organisations have entire team that write and edit the emails they send out, so typos are rare. Scammers do not have that luxury so phishing emails are often laced with typos and grammatical errors.

Some examples of Cybercriminals Defrauding people by using "PM CARES Fund"

After the announcement of PM CARES fund to combat COVID-19 and appeals to citizens to contribute to the fund using digital payment, cybercriminals are taking advantage of this situation to cheat unsuspecting citizens who are eager to help.

They do this by creating fake websites and social media pages as well as through malicious emails and messages that contain fake UPI payment links that sound and are spelt like the official UPI ID which is pmcares@sbi. Some of the **FAKE UPI IDs** include - pmcare@sbi, pmcares@hdfcbank, pmcares@pnb, pmcares@icicibank, etc.

Please note that SBI is the only bank authorised to receive these funds on behalf of the PM CARES fund, so before donating please verify the UPI ID (pmcares@sbi) and the account name (PM CARES) including the exact spelling.

Team Compliance
SMIFS Limited

SMIFS LIMITED
5F, Vaibhav, 4 Lee Road, Kolkata – 700020, India
Tel. No.: (+91 33) 4011 5400 | (+91 33) 6634 5400
Email: helpdesk@smifs.com | Web: www.smifs.com
CIN-U51109WB1993PLC060987