www.isea.gov.in

For more details :
www.InfoSecawareness.in

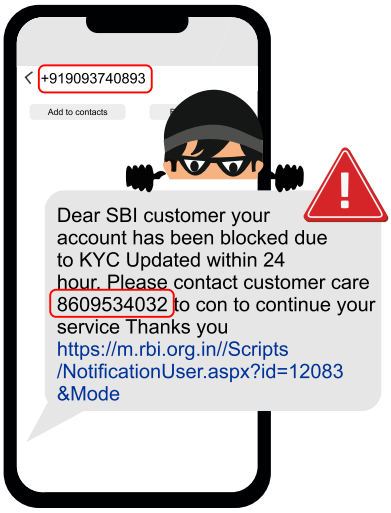
Fraud Alert

Be Aware of the KYC Scam

Targeting the Online Banking Customers

Fake SMS(s) are being circulated, to the banking customers alerting them about the account suspension/block due to pending KYC renewal/update. The fraudsters provide phishing link or fake contact numbers in the message for KYC renewal/update to commit financial scam.

In view of the COVID-19 pandemic, some banks have provided their customers, the facility of updating their KYC online or by post. Taking undue advantage of this provision, the fraudsters are sending fake SMS /text message by pretending to be a bank representative to get your personal details. The fraudsters provide the customers with the phishing link and/or 10 digit mobile number, through which they intend to get hold of customer's personal details to get unauthorized access to their banking accounts to steal money.



Dangers

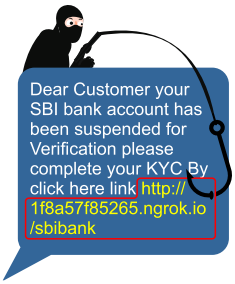
Unauthorized access to account/device/data

Misuse of the personal information

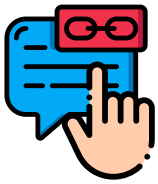
Identity theft

Loss of amount

Modus Operandi



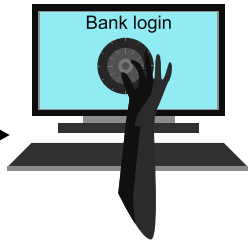
Message sent from a mobile number with a phishing link and/or 10 digit mobile number, for update of KYC.



Upon clicking the link provided in the message, the victim is redirected to the spoofed website and prompted to enter the bank user name, password, OTP etc

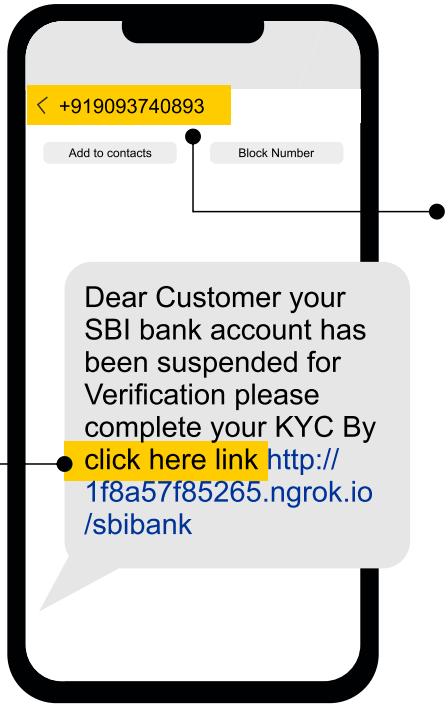
Or

Upon calling the number provided in the message, the victim is provoked to share personal details like account user name, password, account number, OTP etc.,



The fraudster makes use of these details to gain unauthorized access to the victim's bank account to commit fraud

Warning Signs



Poor grammar, punctuation and unwanted capitalization of words in the message received.

Message sent from a mobile number instead of the authorized banking customer care / service number.

Advisory

Never click on unknown links or links received from unverified sources.

Always remember that a bank never sends any links to its customers, for updating KYC.

A valid customer care number can never be a 10 digit mobile number as generally given in the fake message.

Never share your mobile number, account number, password, OTP, PIN or any other confidential details with anyone.

Any authorized bank or customer service never asks its customers to share any confidential information

Avoid contacting the customer service/contact numbers provided on Google search. Only contact the authorized numbers provided in original banking websites.

In case of any such issues immediately report to the specific bank authorities immediately.

File an online complaint regarding any such frauds on the government portal www.cybercrime.gov.in

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

For Virus Alerts,Incident & Vulnerability Reporting
Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

For more details / queries on Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by