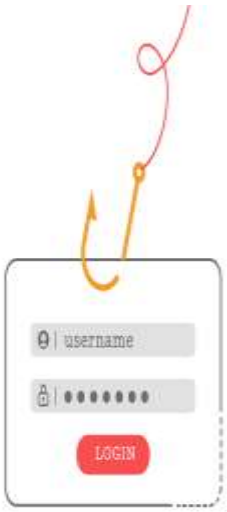
CYBER JAGROOKTA DIVAS – JANUARY-2023

SMS Phishing (Smishing)

A term used to describe a social engineering technique that exploits people via messaging. Attackers send text messages from purportedly trusted companies to trick mobile users into clicking a malicious link or for extracting their personal information.



* BEWARE OF FRAUDULENT SMS

THE NEW PHISHING SCAM:

SMiShing

SMiShing is a phishing attack via SMS, or text messages. These scams try to trick you into clicking a link in a text message. Be wary of unknown texts — and don't click the links!

10 Tips to Avoid Smishing Attack and SMS Fraud

- Do not click on “unknown” messages with links.
- Avoid replying to messages that ask about your finances.
- If in any case, you receive a text message that seems to have come from your bank or the organization you work with, make sure to verify first with the respective legitimate identity.
- If a text message coming from an unknown number urges for a quick reply then it is a sign of smishing.
- Look out for messages that contain numbers like “5000” or any number which isn’t a cellular number. Scammers use these numbers to hide their identities and remain untraceable.
- Never call back the phone number which is associated with the suspicious text message.
- Check the time when an unknown message is sent, as smishing messages are usually sent during an unusual time.
- Messages like “Dear user, you have won…” are the clear sign of a smishing text.
- Always be aware of your bank policies and make sure to stay updated with any change in the policy.
- Keep your organization and business in safeguard by having cybersecurity awareness against such social engineering attacks.