पंजाब एण्ड सिंध बैंक (भारत सरकार का उपक्रम)



Punjab & Sind Bank

(A Govt. of India Undertaking)

Where service is a way of life



CYBER JAAGROOKTA DIWAS

06-09-2023

SMISHING SCAM

Smishing, a blend of SMS and Phishing, is the malicious practice of using deceptive text messages to trick individuals into revealing confidential information, such as credit card numbers, security details, or login credentials.



Latest Smishing example is an E-Challan Scam in which, SMS is received with Fake Challan details and Fake link to Pay the amount.



The victim might be asked to enter sensitive information, such as login credentials, social security numbers, credit card information or personal identification numbers (PINs).



Steps of Smishing

Attacker sends victim a Smishing text message that seems to come from a legitimate source



Once the victim opens and clicks on the link or dials the phone number listed in the message, they're taken to a fraudulent website or a mobile phone line that's designed to resemble a legitimate source.



Message delivers a sense of urgency and compels the victim to take immediate action, such as clicking on a link or calling a phone number.



Threats to Users



- Financial loss due to compromised OTPs and other financial confidential data.
- Loss of Control over your device/mobile.

How To Protect from Scam?



- Always verify the sender of the SMS.
- Never click on links received from strangers or unknown sources.
- Never share your OTP/PIN/CVV to any stranger.
- Do not forward any links or messages without authentication/verification.
- Check official websites of Banks / organizations for official links and customer care numbers.









