Smishing in banking: 3,50,000 frauds happen daily via SMSs

Did you realise that SMS click-through rates are a staggering 20 per cent, compared to email's 3-5 per cent? This disparity has made SMS a prime target for smishing attacks, with an average of 350,000 incidents occurring daily. But why are these attacks so prevalent, and how can we defend against them? What tactics do cybercriminals use to lure their victims, and who are the primary targets? Read here:

"With the widespread adoption of mobile devices for financial transactions, attackers have shifted focus towards targeting mobile users through smishing. This shift is driven by the prevalence of smartphones and the convenience they offer for banking activities," said Shrikrishna Dikshit, Partner- Cyber Security, Nangia & Co LLP.

"Attackers may also gather personal information from publicly available sources such as social media profiles, online directories, and public records. Information can also be obtained by attackers for a modest sum from various sources which have acquired customer data for legitimate purposes but are selling that data for a fee," remarked Shrikrishna Dikshit, Partner- Cyber Security, Nangia & Co LLP.

"Phishing attacks via email or other online channels may precede smishing attempts. In phishing attacks, individuals are tricked into providing personal information through fraudulent emails or websites that impersonate legitimate entities," added Shrikrishna Dikshit of Nangia & Co LLP.