Website Spoofing Scams

Scammers create fraudulent websites that closely resemble legitimate banking websites that are almost identical to the real ones. These fraudulent websites are designed to deceive customers into disclosing sensitive information, including banking login credentials and One-Time Passwords (OTPs).

How the Scam Operates

- Scammers send text messages that individuals have won or have been selected to complete a financial institution through a link provided in the message.
- Clicking the link redirects individuals to a fraudulent website that closely resembles their banking website.
- Unsuspecting individuals enter their banking login credentials on the fake website.
- Subsequently, scammers obtain the ability to access the victims' actual bank accounts.
- The fraudulent website also retrieves the OTP sent from the bank, allowing scammers to gain full access to the victims' bank accounts.

