RBL BANK
apno ka bank

INTERNET & EMAIL FRAUDS (PHISHING)

Internet had made our life convenient with the services such as online banking and shopping but there is always the underlying security risk that criminals will abuse the internet to gain access to our personal banking details and use this to steal our hard earned money.

Fraudsters attempt to acquire information such as usernames, passwords, and other banking details by masquerading as a trustworthy entity in an electronic communication. The act is called as **"Phishing"**.

Phishing is typically carried out by emails or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Safe Banking Tips/Advisory
ATM/Credit Card/ Debit Card/E-Banking
Smishing
Phishing
Vishing
@

Phishers use a combination of **email phishing**, **vishing (voice phishing)** and **smishing (SMS phishing)** to get customer details like account no., login ID, login and transaction password, mobile no., address, debit card grid values, credit card no., CVV no., PAN, date of birth, mother's maiden name, passport no., etc.

How to identify a Phishing attempt?

- Unsolicited emails, calls from strangers or websites asking for confidential banking details
- Messages asking for urgent action due to security reasons
- Links received in emails to access known websites
- To check the actual website, roll the cursor over the link or check for https:// where "s" stands for 'secure site'

Steps to avoid being a victim of phishing attacks-

- Never reply to these emails, and don't click on any links
- Never provide your personal details such as your PIN or account details via email or on any links within these emails.
- Always type banks web site in the address.
- Delete spam emails immediately. Even a request to remove your email address from the mailing list will confirm to the fraudsters that your email account is active, and could open you up to more attacks.
- Never open an email attachment unless you know who sent the message.
- Use the latest browsers which come with filters that alert you when you visit a website that contains potentially unsafe website.

If you come across with any such phishing activity than change your password immediately & report to your branch without any delay.

Your awareness is the key to avoid being a victim of phishing attacks.