Bank AL Habib

Social Engineering

(PHISHING / VISHING / SMISHING)

/BAHLOfficial

SOCIAL ENGINEERING (EMAIL PHISHING / VISHING / SMISHING)

EMAIL PHISHING:

It involves an **E-mail message** appearing to be received from a legitimate organisation. The e-mail requests its recipient to update or verify sensitive information by clicking on a web link redirecting to a fake website or download E-mail attachment.

VISHING:

The **telephone version** of phishing is called Vishing. Fraudsters employ this channel to gain access to important personal and banking information through phone call which leads to data theft and/or financial losses to customers. In stuch cases, the fraudsters often ask the customer to switch-off their mobile phone. This is to keep the customer from knowing about the illegal financial transactions being performed through their Netbanking account.

SMISHING:

Smishing uses **cell phone text messages** to deliver malicious short links to smartphone users through SMS/WhatsApp or any other social media messengers such as Facebook, Signal, Telegram; etc., often disguised as account notices, prize notifications and political messages. Just like phishing, the smishing message usually asks for your immediate attention.

SOCIAL ENGINEERING (EMAIL PHISHING / VISHING / SMISHING)

Don't Take The Bait - **Always spot social engineering attacks** through the following signs:

The Email/SMS will ask you to:

- Provide Username and Password of Netbanking applications
- Provide Personal information (e.g. CNIC, Mother's maiden name, ATM PIN, FPIN, OTP, CVV etc.), for verification or any other purpose
- Download the attachment which may infect your device
- Click web links to access information of particular interest

The Email/SMS containing:

- Wrong spelling
- Grammatical errors
- Have a sense of urgency (e.g., please respond in 48 hours or your account will be locked)

Inspect web-links in an email **by hovering your mouse button over the URL to see where it leads.** Keep in mind phishing email addresses might closely resemble legitimate email addresses.

The caller claims to represent your bank, law enforcement or offer to help you install software or may ask you to provide confidential information.