Subject:- **Surge in Financial/Banking Scams & Prevention (Advisory No. 43)**

Introduction. Recently, a massive increase in banking/financial frauds has been witnessed using phishing and vishing techniques, mainly due to lack of Cyber Security awareness at users' end. Clients of banking sector are continuously falling prey to social engineering tactics and malicious applications looking as legitimate. Accordingly, malicious actors deceitfully withdraw money from users' accounts.

2. **Modus Operandi**. Financial scammers make use of following attack vectors to exploit victim's bank account:

a. **Anonymity**. The attacker's use secure and anonymous cyber means to conduct the operation. Due to which, backtracking is a difficult task.

b. **Social Engineering**. Malicious actors masquerade phone numbers or call from unknown mobile phone/compromised WhatsApp number and masked banking official number to the victim acting as a bank employee/manager and ask for personally identifiable information (Pll) like internet banking username, CNIC number, Debit Card Number and Debit Card PIN. After that the malicious actor tactfully enquires the user whether he/she has received One Time Password (OTP) from bank and asks the user to forward it to the caller directly or by clicking on a WhatsApp link. With this information, malicious actor can easily compromise any bank account and transfer money to potential account/shop online.

c. **Malicious Applications**. The victim receives an SMS containing a link to a phishing website (similar to the banking website or Income Tax Department) where the user is asked to enter personal information, download and install malicious APK file in order to complete verification process. This malicious App masquerades as the Income Tax Department or Internet Banking app. After installation, the app requires user to grant necessary permissions like SMS, call logs, contacts etc. Also, majority of Apps drops key logger malware on victim's device. The acquired data include full name, username, address, date of birth, mobile number, email address and financial details like account number, debit card number and PIN.

3. **Recommendations**. There is no technical solution that can eradicate and detect social engineering; however, safe usage of mobile/computer and compliance with security guidelines is the only way forward. Above in view, cyber awareness campaigns regarding financial scams be arranged at different forums. In addition to it, following protective measures are recommended:

a. Scammers are equipped with latest technology for masking official numbers of banks, users are advised to remain vigilant and call banking helpline themselves, immediately to verify any suspicious call.

b. Never provide sensitive information over phone to anyone, especially passwords, CNIC number and Debit/Credit Card PIN as banks do not ask for such information over phone except when user calls them for activation of debit card or internet banking account.

c. Always pay attention to suspicious numbers that do not look like real mobile phone numbers. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number

d. Beware of false SMS regarding lottery schemes/Benazir Income Support Program prize offers; they are all bogus.

e. Genuine SMS messages received from banks usually contain sender ID (consisting of bank's short name) instead of a phone number in sender information field.

f. All clickable links/ SMS to earn money offers are counterfeit; do not fall prey to them.

g. Never trust and reply anonymous emotional SMS as these are all traps.

h. Always use multi-factor authentication (MFA) on Internet Banking Apps, WhatsApp, Social Media and Gmail accounts.

i. Always keep a strong password for email or online account and regularly change passwords to prevent hacking.

j. Always check application permissions before installation of application and install applications from Google/iPhone Play Store only.

k. Before downloading/ installing apps on Android devices, review app details, number of downloads, user reviews, comments and "additional information" section.

I. Install updated, reputed and licensed antivirus, anti-malware and anti-phishing solutions on PC and mobile devices. After installation, scan the suspected device with antivirus solution to detect and clean infections.

m. Only click on URLs that clearly indicate the website domain. In case of any doubt, users can search for the organization’s website directly using search engines such as Google to ensure that the websites are legitimate.

n. In case of banking fraud, a user should launch complaint to the concerned bank through its Helpline.

o. In case the concerned bank does not take action against the launched complaint within 45x days, a user may launch a written complaint (dully attested by oath commissioner) to Banking Muhtasib of Pakistan on following address:

Banking Muhtasib of Pakistan,
Shaheen Complex, 5th Floor,
MR Kiani Road, PO Box 604, Karachi.