Subject: - **Cyber Security Advisory – Prevention Against Financial Scam Activities - Impersonation as Govt Officials (Advisory No. 53)**

Context. Recently, a substantial rise in banking/financial scams has been observed using **phishing**[1], **smishing**[2] and **vishing**[3] techniques. The scammers introduce themselves as Govt Officials (FIA, SBP and Defence Force using fake official landline numbers and logos on WhatsApp DP) through call-cloning services. Resultantly, online-banking users continuously fall prey primarily due to lack of cyber security awareness, as well as advanced social engineering tactics used by scammers (call cloning, malicious apps and fake websites). As a result, malicious actors deceitfully withdraw money from user's accounts

2. **Scammers Working Model**. Financial scammers make use of the following attack vectors to exploit victim's bank account:

a. **Fake Websites – Reference of Army Poverty Alleviation Campaign**. Scammers are using spoofed websites appearing to be State Bank of Pakistan legitimate verification website and asking victims to upload personal financial details on website in reference to Pakistan Army Poverty alleviation and Revival of Economy Campaign. Fake website of State Bank of Pakistan for verification being referred is **(www.statebankverificaiton.wixsite.com)**

b. **Social Engineering**. Malicious actors masquerade phone numbers or call from unknown mobile phone/compromised WhatsApp number, masked banking official number to the victim acting as a bank employee/manager and ask for personally identifiable information (PII) like internet banking username, CNIC number, debit card number and debit card pin. After that the

[1] **Phishing** is fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

[2] **Smishing** is fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

[3] **Vishing** is fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

malicious actor tactfully enquires the victim 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. Armed with this information, malicious actor can easily compromise any bank account and transfer money to potential account or perform online shopping.

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

3. **Recommendations**. There is no technical solution that can eradicate and detect social engineering completely; 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. Blocking of fake website appearing to be state bank verification website **(www.statebankverificaiton.wixsite.com)**
b. 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.
c. 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.
d. 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.
e. Be aware of false SMS regarding lottery schemes/Benazir Income Support Program prize offers; they are all bogus.
f. 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.

g. All clickable links/SMS to earn money offers are counterfeit; do not fall prey to them.
h. Never trust and reply anonymous emotional SMS as these are all traps.
i. Always use multi-factor authentication (MFA) on Internet Banking Apps, WhatsApp, Social Media and Gmail accounts.
j. Always keep a strong password for email or online account and regularly change passwords to prevent hacking.
k. Always check application permissions before installation of application and install applications from Google/iPhone Play Store only.
l. Before downloading/installing apps on Android devices, review app details, number of downloads, user reviews, comments and “additional information” section.
m. 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.
n. 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.
o. In case of banking fraud, a user should launch complaint to the concerned bank through its Helpline.