Subject:- **Advisory - Prevention against Social Engineering Techniques through Facebook (Advisory No. 30)**

1. **Context.** Recently, data of **533 million Facebook users** has been posted online which includes **User IDs, full names, birth dates, gender, location** and **job status** etc. The data was accessed through a **Telegram bot.** The data leak incident has necessitated to take protection measures against social engineering attacks facilitated by **Personally Identifiable Information (PII)** posted online. Social media users are also required to take stringent security and privacy measures to protect against any future data leaks revealing **Personally Identifiable Information (PII).** It is recommended to follow remedial actions mentioned in ensuing paragraphs for safeguards against Social Engineering attacks and protection of personal information while using Facebook and other online services.

2. **Safeguards Against Social Engineering Attacks**

a. **Sharing Private Information Online.** Never share private information on any online platforms. During online shopping credit card information must only be entered on secure platforms / websites using https protocol. Login credentials and passwords must never be shared.

b. **Unknown / Spam Email.** Beware of unknown emails and links sent on social media platforms. Links forwarded by unknown senders may never be clicked. Moreover, spam filter must always be enabled for automatic categorization of suspicious links.

c. **Password Management.** Implement complex password policy by using special characters to avoid dictionary attacks and never use same passwords on all platforms.

d. **Multifactor Authentication.** Use multifactor authentication to avoid possible hack / data breach even if password is compromised.

e. **Monitoring of Online Accounts.** Periodically monitor online bank accounts to ensure that no un-authorized transactions have occurred.

f. **Limited Personal Information.** The best policy while using Social Networks is not to trust anyone and only reveal minimum possible information.

g. **System Update.** Keep Operating System (OS), browser, Antivirus (AV) protection and firewalls up-to-date to safeguard against exploits affecting personal information.

h. **Encryption.** Personal data stored on systems must always be encrypted.

i. **Awareness.** Incorporating continuous training / awareness campaigns to consistently apprise HR against latest Social Engineering threats.

3. **Protect Personally Identifiable Information (PII) on Facebook**

a. **Removing Profile from Search Engines.** Tap the icon with the three

lines in the top right menu > Settings & Privacy > Settings > Privacy > Edit Option "Do you want search engines outside Facebook to link your profile" and Select No.

b. **Highest Security Settings.** Frequently check your security settings as they are.

c. **Sharing Personal Information.** Use "Custom Privacy Settings" to make personal information private. Date of Birth, Family details and address must be removed / edited to protect identity theft.

d. **Login Alerts.** Check your login alerts frequently to ensure there are no un-authorized logins to account.

e. **Deny Location Access.** Tap the icon with the three lines in the top right menu > Settings & Privacy > Privacy Shortcuts > Manage your location settings > Location Access. Switch the toggle for Background Location to Off.

f. **Two-Factor Authentication.** Go to Settings > Security and Login > Use two-factor authentication.

g. **Privacy Checkup.** Run a privacy checkup to review your current privacy and sharing settings. Following things can be reviewed in privacy settings

(1) Limiting people that can see certain information on your profile.

(2) Updating passwords and turning on alerts.

(3) Limiting people that can send friend requests or search on facebook.

(4) Limit audience for current and past posts.

(5) Privacy settings can also be reviewed for various apps and games.

* * * * *