Subject: **Advisory-Safe Usage of Mobile Phone to Avoid Hacking (Advisory No. 17)**

Background. Mobile phones continue to expand in their popularity and usage, blending the functions of the personal computer and telephone. Mobile phone security has become increasingly important now days. Secure use of mobile phone is of particular concern as it relates to the security of personal and business information.

2. **Vulnerabilities of Mobile Phones**

a. When there is an attack, there must be some vulnerability. Mobiles are preferred target of attackers. Attackers exploit weaknesses related to smart phones that can come from means of communication like SMS, MMS, Wi-Fi networks, Bluetooth and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. There are malicious software, which rely on the weak knowledge of average users.

b. While using mobile phone user is exposed to various threats. These threats can disrupt the normal operations and transmit or modify the user data. For these reasons, installed applications must guarantee privacy and integrity of the information they handle. In addition, some apps could themselves be malware, their functionality and activities should be limited (for example, restricting the apps from accessing location information via GPS, blocking access to the user's address book, preventing the transmission of data on the network etc.).

c. **Prime Targets for Attackers**. There are three prime targets for attackers:-

(1) **Data**. Mobiles may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs).

(2) **Identity**. Most people are using smart phones now a days. These smart phones are highly customizable; attacker can access the identity details of user, for further criminal offenses.

(3) **Availability**. By attacking a mobile phone, one can limit access to it and deprive the owner of the service.

3. **Indicator of Compromise (IoC)**. Following checklist necessitates to see if mobile has been hacked:-

a. Over usage of internet/data of mobile phone by specific apps.
b. Communication with suspicious command and control servers (check via network log analysis).
c. Overheating of mobile phone.
d. Rapid battery draining.
e. Blocking of Social media apps and inaccessibility to log in.
f. Sudden loss of networks and data wiping.
g. Calls/messages being delivered to contacts without user's interaction.

4. **Measures to Improve Security/Prevent Hacking of a Mobile**. Following measures are suggested for using mobile phones: -

a. **Connect with care**
   (1) When using public and insecure wireless hotspots and Wi-Fi, avoid visiting sites that require PII such as name, locality, CNIC, number, passwords, credit card numbers etc.
   (2) **Wi-Fi Router Security**.The default configurations of most of the routers offer little security. Though it may seem cumbersome to spend time configuring the router's settings, it's well worth it, because a secure router is one of the best initial line of defense. Compromised router may result in hacking of your mobile. To secure the router, its user guide be consulted, which will direct the browser to a predefined URL or IP address where you can do the following: -
      (a) Configure the wireless network to use WPA2-PSK with AES encryption for data confidentiality.
      (b) Wi-Fi password must be complex and at least 15 characters long
      (c) Chang the default login username and password.
      (d) Conduct MAC address filtering (a form of white listing or identifying wirelessly connected computers).
      (e) Change the default wireless SSID.

b. **SD Card Protection**. In the same way as on a computer, SD card protection is very important in mobiles. Never give your SD Card to any one and always use a password to protect it.

c. **Remove Unnecessary Applications**. Intruders can attack mobiles by exploiting software vulnerabilities. Less applications installed in phone, there are less chances of potential attacks. Keep mobile software and all the apps up to date. Always install apps from authorized stores, which are mentioned below:-

(1)	IPhone	-	iTunes Apple Store
(2)	Android Phones	-	Google Play
(3)	Huawei Phones	-	Huawei App Store
(4)	Windows Phone	-	Windows App Store

d. **Remove Unnecessary Permissions for Apps**. Check and allow only necessary permissions of each app while installing on phone. A number of applications e.g. loan lending apps actually extract data from phones discreetly without user's knowledge.

e. **Anti-Phishing Measures**
   (1) Never open any attachments from unknown sources/senders.
   (2) If any link or email seems suspicious, just ignore it; even don't try to unsubscribe it by clicking unsubscribe link as it may allow hacker to access your emails data.
   (3) If any suspicious message is received, immediately consult IT Administrator of your organization.

f. **Avoid Visiting Insecure Websites on Mobile Web**. Never open HTTP sites on mobile web. Also, avoid visiting suspicious websites

including adult websites as majority of them redirect to malicious websites/attachments resulting in hacking of device.

g. **Lock Your Device with Password**. Always lock your device with a strong PIN:-
   (1) To ensure phone security, always use strong passwords by employing combination of alphanumeric, special characters, upper- and lower-case letters.
   (2) For PIN, avoid using general and easily guessable passwords e.g. DOB, own/family names, vehicle registration number etc.
   (3) Keep your PIN or password private.
   (4) Regularly change your password and do not keep same password for multiple phones and apps.

h. **Apply Antivirus Updates**
   (1) Use well reputed and licensed anti-viruses and anti-malwares.
   (2) Avoid using free anti-viruses. Majority of those are actually malwares and data scrapping apps.
   (3) Most antivirus vendors release updates to patch or fix vulnerabilities, flaws and weaknesses in their software. Because intruders can exploit these bugs to attack a computer. Keeping the software updated is important to prevent infection.
   (4) Intruders can set up malicious websites that look identical to legitimate sites. Only download app updates directly from a vendor's website, from a reputable source, or through automatic updating.

i. **Network Monitoring**. Proactively monitor network usage and connections with other APIs through trusted software's. In case of any suspicious activity, consult IT expert or administrator.

j. **Use GPS Features Wisely**
   (1) Limit the apps that allow tracing the location via GPS.
   (2) Think before you turn on Geo-tagging for taking snaps and pictures.

k. **Security Features**. Following security features must be enabled in phone:-
   (1) Finding and remotely wiping the device.
   (2) File encryption.
   (3) Encrypting offline backup.
   (4) Access camera/microphone.

l. **Before Disposing Off the Phone**. Delete all information stored in a device prior to discarding it. In addition, it is advisable not to sell SD Card along with the phone as deleted data can be recovered from them. Never sell your used phone in market. If not in use, ensure destruction of handset.

m. **Act Quickly if Mobile is Stolen**
   (1) Report the loss of mobile to police.
   (2) Report to service provider for SIM blocking.

(3) Immediately change the login credentials of all accounts in the mobile.

(4) Use features like remote wipe to remove data.

n. **Limit Access to Contacts**. Never synchronize contacts with online services. IPhone provides the capability to limit applications from accessing the contacts however android phones still lack this option as a built-in feature.

o. **Personal Data**. Carefully consider what information is kept on the device as access to the phone for short time can allow hacker to extract the personal data from the smartphone.

p. **Secure Surfing**. Do not follow links sent in suspicious email or text messages.

q. **Free Wi-Fi Hotspots**. Free Wi-Fi provided at hotels, cafés and airports should not be used.

r. **Rooting or Jail Breaking**. Do not "root" or "Jailbreak" the device. As custom firmware has no authenticity of being clean from malware and can be used to freely access the mobile.

s. **Physical Safety**. Never leave the phone unattended as malware can be easily installed in the phones.

t. **Publicly Available Power Charging**. Publicly available USB charging slots are used for seamlessly copying data from the phones. Therefore, they must be avoided.

u. **User Awareness and Alertness**. Periodic cyber awareness campaigns to establish firm alertness regarding safe usage of mobile phones is the ultimate preventive measures, above all other best practices.

5. **Steps to Avoid Data Leakage in Case of Breach**

a. Official/sensitive data be stored in encrypted form with no direct public access.

b. Never store official data and family/private data on your phone.

c. Never use personal phone and Email for official communication. Always use separate/official channel for official correspondence.

d. Do not discuss secret official matters on call/SMS/landline/ GSM/WhatsApp etc. use officially dedicated communication numbers.

e. Avoid using free and lucrative apps as majority of them steal data from PC and mobile phones.

f. Do not use cracked versions of software. Always install paid software from official support and store.

g. Do not share official documents via WhatsApp, Telegram, Messenger and other so-called end-to-end encrypted messaging apps/secret chatting applications as their servers are hosted outside Pakistan.

h. Do not use online PDF Scanner apps. Only scan secret documents via official hardened scanners.

i. Cover the cameras of phone with tapes/stickers, when not in use.

j. Never take mobile phone in meeting room, office and other restricted areas.

k. Never store passwords in mobile notes.
l. Never store important official commitments in calendar.
m. Always add contact name with confusing names to avoid PII exposure of VIP contacts in case of breach.