

5

**GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)**

No. 1-5/2003 (NTISB-II)

Islamabad 29 August, 2018

Subject: Advisory - Prevention Against Ride Sharing Services (Advisory No 155)

- Context.** Due to high prices of transportation in Pakistan, use of **online ride sharing services** (Uber, Careem) has exponentially increased in the last few years. Despite numerous advantages, these online ride sharing services poses a **serious threat to privacy and security** of users.
- These firms have also suffered many **security breaches** resulting in leakage of end user data. M/s **UBER** concealed a **massive global data breach** of the personal information of **57 million** customers and drivers in year 2017.
- Technical Analysis/ Permission Used By Apps.** Extra permissions are being acquired by ride sharing applications, which can be used for malicious purposes. Detail of permissions asked by these apps is as under:-

Ser	Name of App	Type of Permission	Operational Requirements	Lurking Threats
a.	Uber	Identity	Essential	Apps can use sensitive data from authorized accounts
		Wi-Fi Info	Essential	-
		Device ID	Essential	Can expose IMEI numbers
		Location	Essential	Threats arise from location based ads or malware attacks
		Contacts	Not Essential	Gain unnecessary access to contacts.
		SMS	Not Essential	Send illegitimate texts
		Phone	Not Essential	Can be used secretly to call numbers
		Photos/Media/ Files	Not Essential	Data/ recordings can be stolen, deleted or shared
		Camera	Not Essential	Take unwanted pictures
b.	Careem	Location	Essential	Threats arise from location based ads or malware attacks.
		Wi-Fi Info	Essential	-
		Device ID	Essential	Can expose IMEI numbers
		Photos/Media /Files	Not Essential	Data/ recordings can be stolen, deleted or shared
		Camera	Not Essential	Take unwanted pictures

4. Preventive Measures.

- Disable all unnecessary permissions** mentioned at **Para 3**. Steps for disabling permissions in android operating system are mentioned below:-

PS TO CHIEF SECRETARY SINDH
Diary No. 22769 18
Inward Date 3/9/2018
Outward Date

NO. PS/SECY/I.T/203 DG IS&IT Dairy No. 288
Dated: 06.08.2018
Dated: 7/9/18

(I.T)/Transport/Horme/b/A

7/9/18

7.9.18

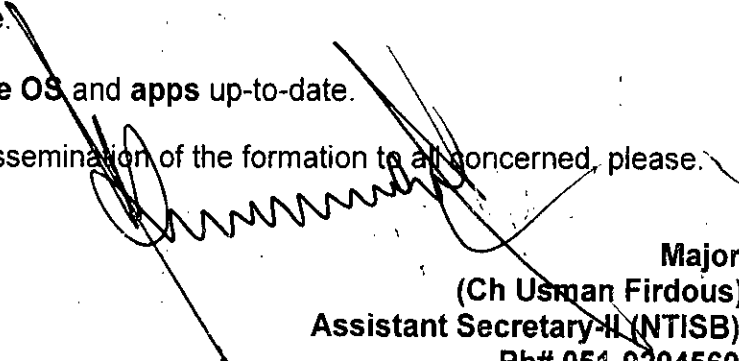
Director
DDCT

7/9

Sr. Manager (Tech/Policy)

Sr. Manager (Tech/Policy)

- L.I.
- (1) Open the main **settings** app.
 - (2) Tap **Apps** or **Application manager**.
 - (3) Tap the desired app for update.
 - (4) Tap **Permissions**.
 - (5) Turn Permissions on or off.
- b. **Close app** when they are not in use.
- c. Download apps from **Google's Official Play, Store** vigilantly and always verify **app permissions** and reviews before downloading any app.
- d. Enable Google Play Protect security feature on the device. This feature will remove (uninstall) **malicious apps** from user's Android smartphone to prevent further harm.
- e. **Turn off** app installation from **Unknown sources**.
5. **Recommendations.** In order to prevent user's data from being vulnerable to theft, following is suggested:-
- a. Strictly follow all **mitigation measures** mentioned at **para 4**.
 - b. Install an **antivirus app** (e.g. Avast) on smartphone that can detect and block malicious apps before they can infect a device.
 - c. Always **review app permission** before installing any app on Android/ iOS based smart phone.
 - d. Always keep the **device OS** and **apps** up-to-date.
6. Forwarded for perusal and dissemination of the formation to all concerned, please.


Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments

Copy to :-

SPS to Cabinet Secretary, Cabinet Division, Islamabad

PS to AS-III, Cabinet Division, Islamabad

APS to Secretary, NTISB

APS to Deputy Secretary, NTISB

Handwritten notes and signatures:
20. Mr. M. (NTISB) [Signature]
RIF
[Signature]
[Signature]
[Signature]