

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

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

Islamabad 20 July, 2018

Subject: Cyber Security Advisory - Hacking of Social Media Accounts  
(Advisory No 139)

1. **Context.** Cyber has emerged as fifth domain of warfare by radiating threat in entire spectrum of conflict (peace & war). Organizations dealing with public/ private sector maintain their **presence** on **social media/ internet** through their official websites and accounts. However it has been observed that, there is a **rise in hacking of social media accounts** since last 1 x year due to **lack of awareness** on usage of internet & mobile.

2. **Threats Posed by Hacking of Social Media Accounts**

- a. **Hostile quarters** can easily map the **real identities of officers/ staff** of an organization for conducting **subversive activities**.
- b. Personal emails/ numbers posted on official websites is the biggest source for **hacking and data breach**.
- c. Hacked social media can be used to access friends, family and colleague of **senior Govt officials**.

3. **Preventive Measures for Security of Social Media Accounts.** Following preventive measures are suggested in this regard:-

- a. Anything **posted on social media** cannot be **completely deleted**, so it is advised to be vigilant while creating any activity.
- b. Never use **free WiFi available** at airports, hotels, shopping malls etc.
- c. **Public profile** information creates a goldmine of info for hackers; therefore effort must be exercised to limit audience.
- d. Utilize all **security settings** available by the social media platforms for **security** of users.
- e. It is strongly **recommended** to use **2 factor authentication** for logging in social media account.
- f. Following best practices should be followed for **password management**:-
  - (1) **Change the passwords** of social media accounts on **regular basis**.
  - (2) Always use the password in combination of characters, upper/ lower case, letters and numbers.
  - (3) Avoid **reusing** the same password.
  - (4) Never use same password for multiple accounts.
  - (5) Always **memorize the passwords**, never write it.

- g. Never create multiple social media accounts on single email address.
  - h. Manage your **privacy settings**.
  - i. Messages received on **Facebook, Twitter** and **LinkedIn** should be strictly scrutinized.
  - j. Be very vigilant on **social media groups** and **don't click** on any link being shared by any known/ unknown group member.
  - k. Be selective while **accepting a friend request** and make sure that it is **real/ actual profile**.
  - l. Be aware of the fact that the **information you share on any social network** may be linked to another platform.
  - m. **Turn off GPS function** on your smart phone camera.
  - n. Don't enable **auto login**.
  - o. **Close all unused accounts and** delete as much **personal information** from them as possible.
  - p. Avoid using **online applications** that require access to your personal Or profile information.
  - q. Avoid mentioning **work place** as the information can be used for **social engineering**.
4. **Recommendations.**
- a. **Download apps** with vigilance not only from the **third-party app store'** but also from official Play Store.
  - b. Regularly check the vendor website for' **updates** and **release of security, patches** of all operating systems/ software's deployed.
  - c. Strictly follow **mitigation measures** mentioned at **para 3** for security of **social media accounts**.
  - d. **Caution the aware employees** on **safe social media** usage and basics of **cyber security**.
5. Forwarded for perusal and dissemination of information to all concerned, please.

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

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