

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

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

Islamabad 2 January 2019

Subject: Advisory - Prevention Against Cyber Espionage (Advisory No.1)

*04 JAN 2019*  
*M(A)*  
*M(I.T)*  
*A.S (Rev. Div.)*

**Context.** Hostile actors are utilizing Google web hosting service (<https://sites.google.com>) for hacking gmail accounts. The generated phishing / fake link looks valid and legitimate due to prefix (https) and suffix (google.com). Internet users are advised to be **mindful of this hacking attempt as currently it has very low detection rate and it can be used easily for targeted attacks with no track back.**

**2. Summary of Cyber Attack**

- 7 JAN 2019*  
*C(A)*
- (A.S.)*
- a. Malicious emails containing phishing links with fol subjects are being sent by the hackers.
    - 1) Sign in from unknown device in Syria
    - 2) Gmail Account verification.
    - 3) Unknown sign in attempt from Uruguay.
  - b. **Phishing Link** ([https://sites.google.com/view/\[.xxx\]](https://sites.google.com/view/[.xxx])). It is hard to identify the phishing page as it looks close to real. Screen shot is attached at **(Anx A)**.
  - c. **Purpose:** To **steal credentials** i.e. email accounts, phone numbers, recovery account information etc from internet users in general and **internet users of sensitive organization in particular.**

**indicators of Compromise.** Following indicates whether phishing attempt has backed the email account or not.

- S. (Copy)*  
*7/1/19*  
*4.*
- a. Unable to log into gmail account
  - b. Unable to recover gmail account via mobile phone and other devices.
  - c. Hacking of social media and banking accounts associated with that email address.

**Method of Operation.** Following is the method of infection that enables hackers to steal credentials of email:-

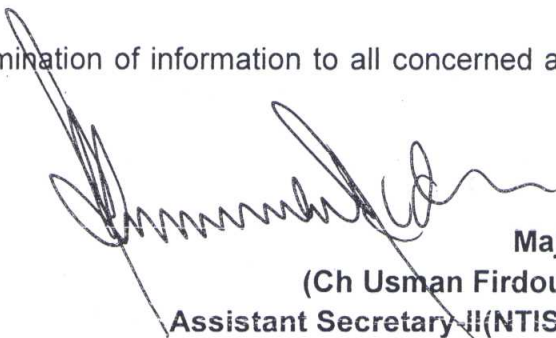
- a. The user receives a **legitimate looking spoofed email from google** ([services.secure.info@gmail.com](mailto:services.secure.info@gmail.com)) stating that an unknown sign-in attempt has occurred from a different country.

- b. User is asked to click on the link and enter current user name & password, along with personal mobile phone number and recovery email address to verify his identity and email account.

5. **Recommendations.** In order to enhance security against attempts of phishing, following is suggested:-

- a. **Avoid spoofed emails / subjects** and mark them as spam and forward them to emails mentioned in para 5 ante for further inspection.
- b. **Don't login on links forwarded to you via email and always authenticate URL before signing in.**
- c. **Install well reputed antivirus software** like Kaspersky, AVAST etc that can block known phishing sites.
- d. Enable **"Two Factor Authentication"** in all personal email accounts especially those linked with social media sites and internet banking.
- e. **Utilize well reputed browsers** like Chrome and Firefox and don't install **unnecessary browser plugins or addons** except from adblock or adblock plus.
- f. **Don't click on popups and ads** displayed during web browsing.

6. Forwarded for perusal and dissemination of information to all concerned and under command, please.



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

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Government.**

1. SPS to Cabinet Secretary, Cabinet Division Islamabad
2. PS to AS-III, Cabinet Division Islamabad
3. APS to Secretary, NTISB
4. APS to Deputy Secretary, NTISB

