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

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

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]). 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**.

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

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.

4. **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) 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 verity 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**.

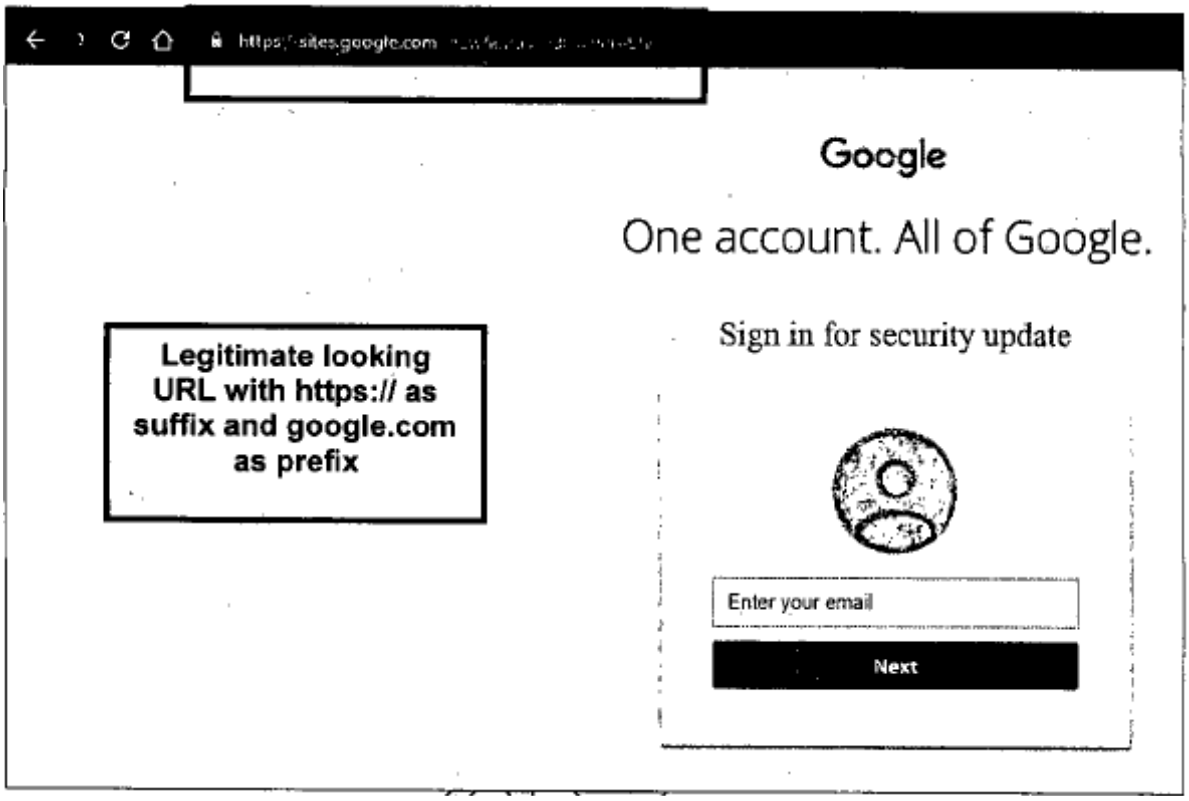
c. **Install well reputed antivirus software** like Kaspersky, AVAST etc that can block known phishing sites.

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 clock on popups and ads** displayed during web browsing.

Annex-A


Google
One account. All of Google.
Sign in for security update
Enter your email
Next
Legitimate looking URL with https:// as suffix and google.com as prefix