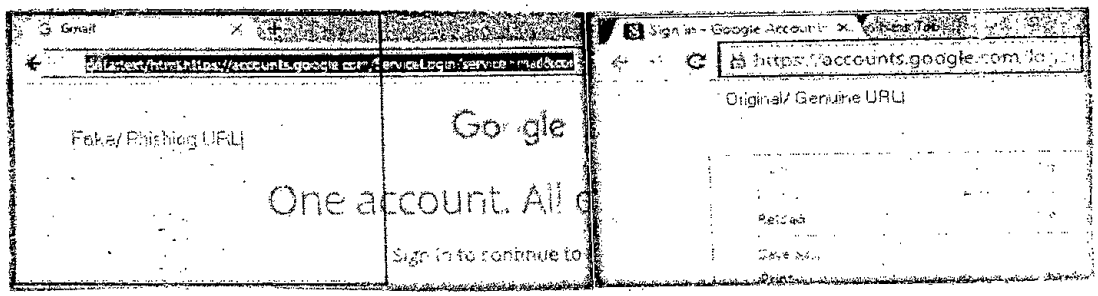
Subject: **Guidelines for Prevention Against Phishing Attacks / Scams Related to Trending Topics i.e. Coronavirus (COVID-19) and China-India Border Conflict (Advisory No. 15)**

1. **Introduction.** Recently, threat actors have been taking advantage of the interest surrounding trending topics such as COVID-19 and the border conflict between India and China to trick users into clicking on / downloading malicious email links and attachments in order to attack and invade corporate networks. Hostile elements spoof / impersonate email addresses to look legitimate. It is advised to follow instructions in para 2 to safeguard against phishing exploitation.

2. **Recommendations** Following are recommended measures against phishing attacks: -

a. Always check complete URL before providing login credentials or clicking on a link and make sure that its https:// with no spelling mistakes in address.



b. Don't download **email attachments from untrusted sources or unfamiliar addresses.**

c. Remain vigilant for **scams related to trending topics such as Coronavirus Disease 2019 (COVID-19),** or **China-India border conflict** as attackers may send emails with malicious attachments or links to **trick victims into revealing sensitive information**

d. Download software applications form trusted source only. Especially abstain from **downloading / installing applications sent through SMS / WhatsApp messages.**

e. Install licensed and **updated well-reputed anti-virus software**.

f. Enable **personal / domain firewalls** on workstations.

g. **Harden web browsers** to block execution of JavaScript and Adobe Flash which is used for most attacks on privacy.

h. **Disable macros permanently**, as victims are actively targeted using macro based malware.