Subject:- **Phishing Email for Stealing Username / Password (Advisory No. 07) April 2015**

Recently, several emails have been reported and evaluated that show a new trend in fake/phishing emails for **stealing username/password** of targeted users.

2. **Modus Operandi.**

   a. Emails is sent using fake IDs which impersonate official address of service provider such as Gmail, Hotmail etc.

   b. Subject of the email tricks, lures or forces the user into entering username / password on fake login pages thereby stealing the information.

   c. **Known / Reported Incidents**. Some of the significant reported imidusance given below:-

Ser	Subject of Email	Email Sender impersonating Official Address	Annex
(1)	Update your personal information	google.service.manager@gmail.com	Annex A
		google.update.notification@gmail.com	Annex B
(2)	Unusual activity on your mail account	serive_ update_team@outlook.com	Annex C
(3)	Warning	do_not_repply@hotmail.com	Annex D
(4)	Violation of e-mail security	google. update.nitificatio@gmail.com	Annex E
(5)	Distrustful sign in from Israel stopped	google. update. notification@gmail.com	Annex F
(6)	Google Security: Access for apps has been enabled	no_reply@accounts.google.com	Annex G
(7)	Multiple login Attempts	service.updates.team@gmail.com	Annex H

3. **Recommendations**. In order to enhance security against attempts to steal passwords following is suggested, please:-

   a. .Avoid checking such spoofed e-mails/subjects and mark them as spam.

   b. Such emails may be forwarded on following email address for analysis and suggesting their authenticity. Coordination may also be carried out at 051-9204560 for immediate action:-

         (1)   eagle 1978@mail.com

         (2)   falcon098@writeme.com

c.   Install well reputed antivirus / firewall software that block known phishing sites:-

         (1)   Bit defender Total Security.

         (2)   Kaspersky   Internet Security.

         (3)   Eset NOD32 Internet Security

d.   Change password of the account immediately

e.   Enable "Two Factor Authentication" in all email accounts. As en example, procedure for enabling it in gmail is att as Annex I.

f.   Before entering username and password on login pages, please ensure that the action is being carried out on actual pages. Verify the address in "address bar" of web browser as mentioned at Annex J.

g.   Use chrome or firefox and install plugin" Web of Trust" to view rating of page before opening it.