GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)
***

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

Islamabad 6 May, 2015

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:-,

Page contd...2

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

b. Such emails may be forwarded on following email address for ana and suggesting their authenticity. Coordination may also be carried ou 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 sit

(1) Bitdefender 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 exar procedure for enabling it in gmail is att as Annex I.

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

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

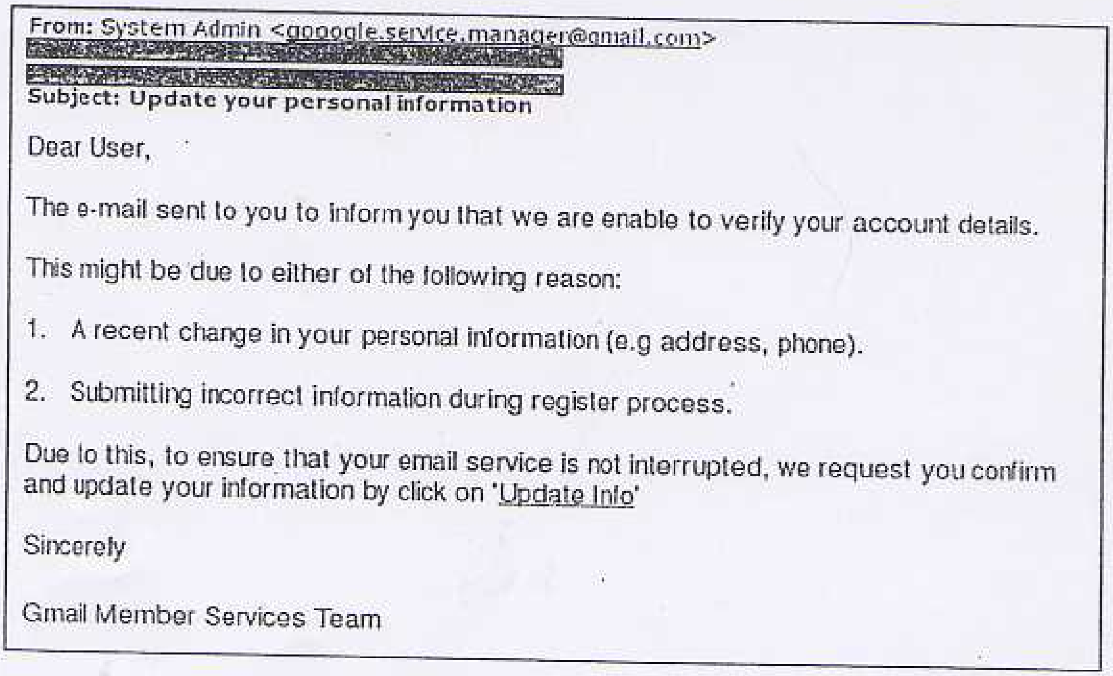
4. It is requested that above mentioned information may be disseminated t concerned in order safeguard against leakage of sensitive information.

M
(Iftikhar
Assistant Secretary (NT
Ph # 051-920

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

Anx A

Phishing (Fake Email) - 01



From: System Admin <gooogle.service.manager@gmail.com>

[redacted]

Subject: Update your personal information

Dear User,

The e-mail sent to you to inform you that we are enable to verify your account details.

This might be due to either of the following reason:

1. A recent change in your personal information (e.g address, phone).
2. Submitting incorrect information during register process.

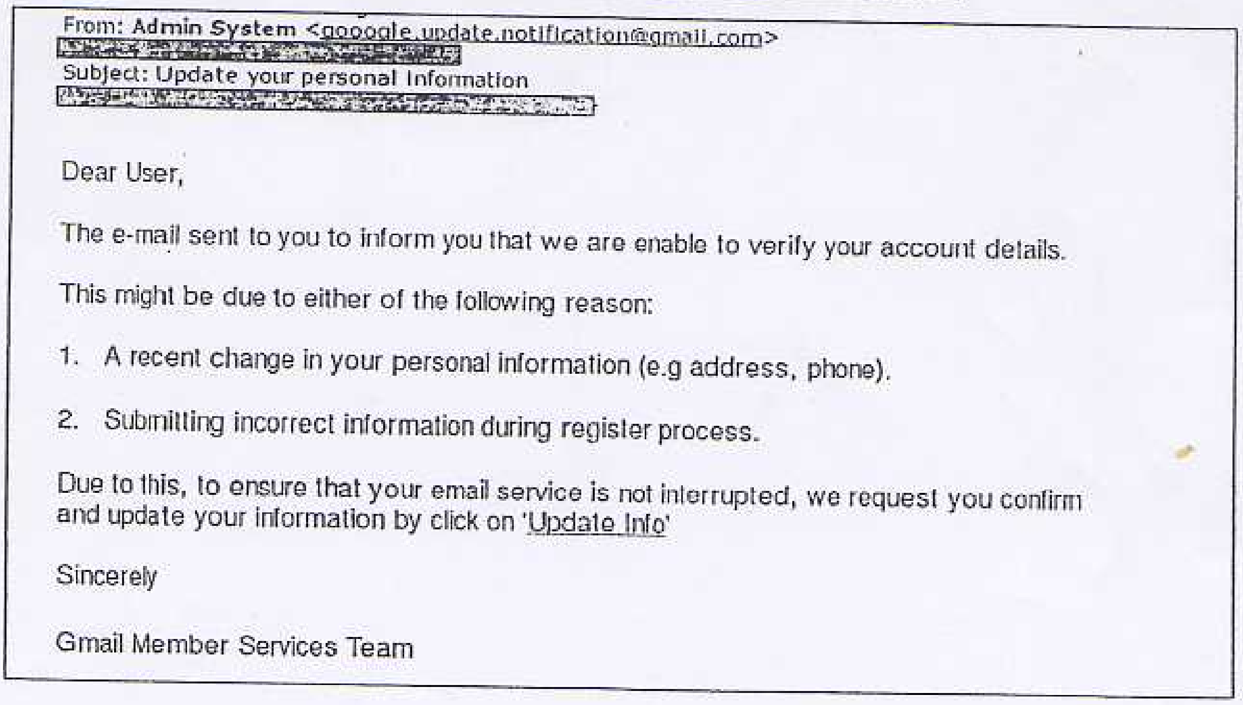
Due to this, to ensure that your email service is not interrupted, we request you confirm and update your information by click on 'Update Info'

Sincerely

Gmail Member Services Team

Anx B

Phishing (Fake Email) - 02



From: **Admin System** <gooogle.update.notification@gmail.com>

[redacted]

Subject: Update your personal Information

[redacted]

Dear User,

The e-mail sent to you to inform you that we are enable to verify your account details.

This might be due to either of the following reason:

1. A recent change in your personal information (e.g address, phone).
2. Submitting incorrect information during register process.

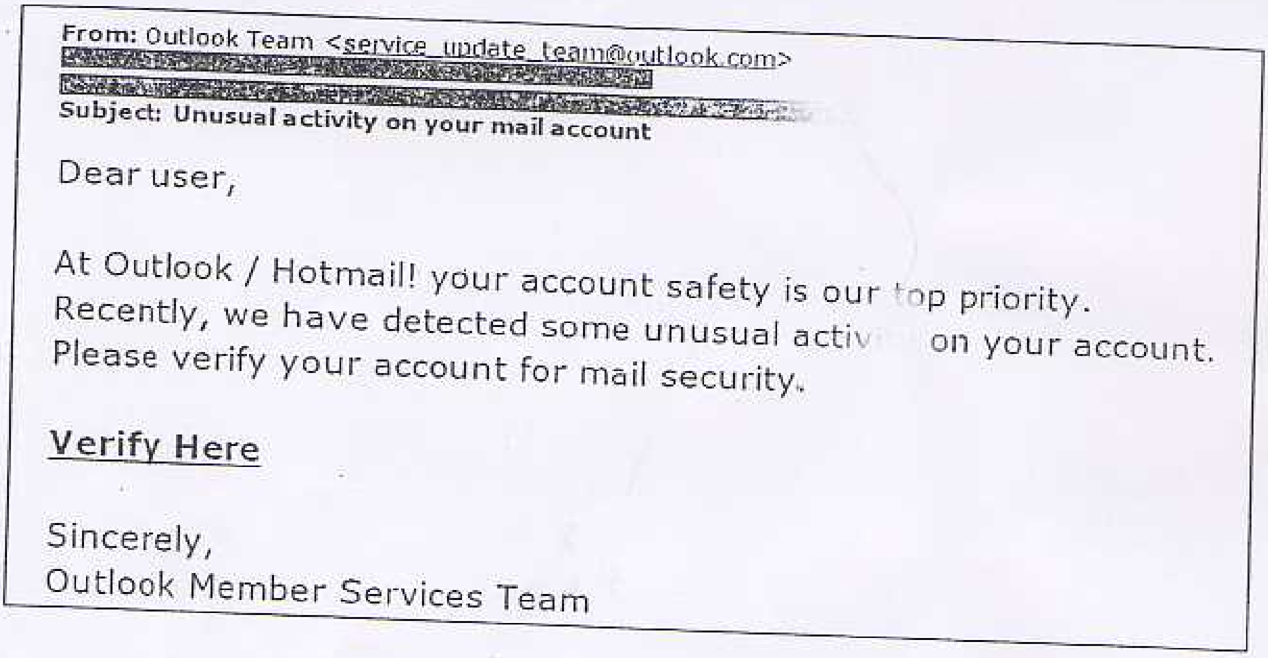
Due to this, to ensure that your email service is not interrupted, we request you confirm and update your information by click on 'Update Info'

Sincerely

Gmail Member Services Team

Phishing (Fake Email) - 03

Anx C



From: Outlook Team <service_update_team@outlook.com>
[redacted]
Subject: Unusual activity on your mail account

Dear user,

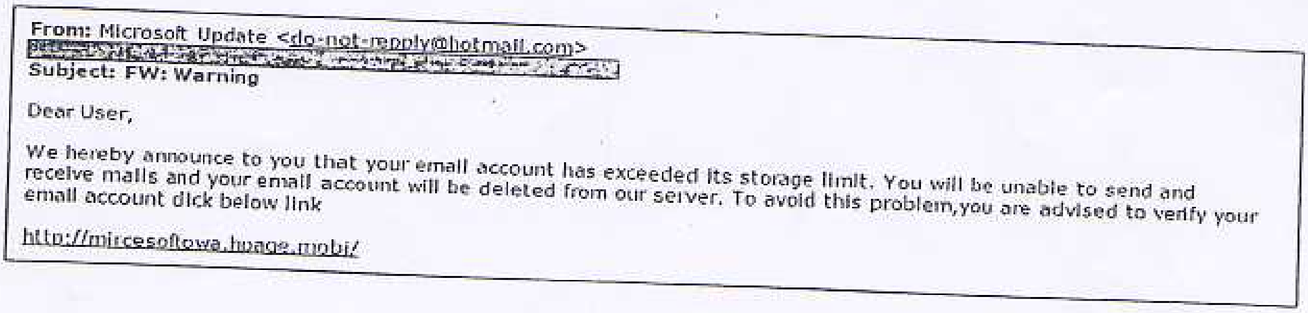
At Outlook / Hotmail! your account safety is our top priority. Recently, we have detected some unusual activity on your account. Please verify your account for mail security.

Verify Here

Sincerely,
Outlook Member Services Team

Phishing (Fake Email) - 04

Anx D



From: Microsoft Update <do-not-repply@hotmail.com>
[redacted]
Subject: FW: Warning

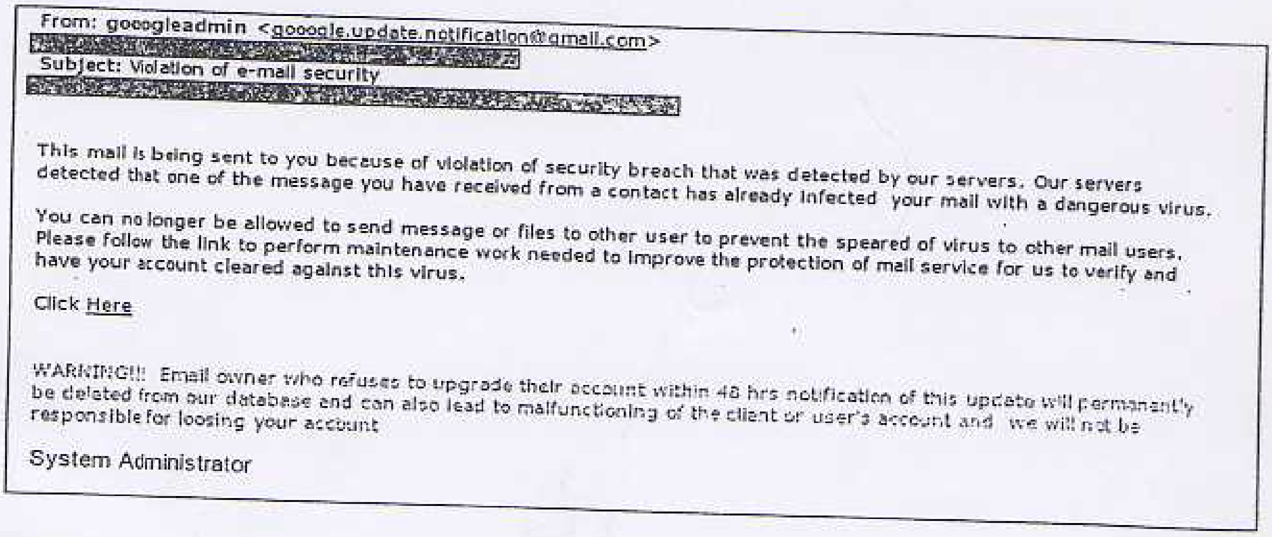
Dear User,

We hereby announce to you that your email account has exceeded its storage limit. You will be unable to send and receive mails and your email account will be deleted from our server. To avoid this problem,you are advised to verify your email account dick below link

http://mircesoftowa.hpage.mobi/

Anx E

Phishing (Fake Email) - 05



From: gooogleadmin <gooogle.update.notification@gmail.com>

[redacted]

Subject: Violation of e-mail security

[redacted]

This mail is being sent to you because of violation of security breach that was detected by our servers. Our servers detected that one of the message you have received from a contact has already infected your mail with a dangerous virus.

You can no longer be allowed to send message or files to other user to prevent the speared of virus to other mail users. Please follow the link to perform maintenance work needed to improve the protection of mail service for us to verify and have your account cleared against this virus.

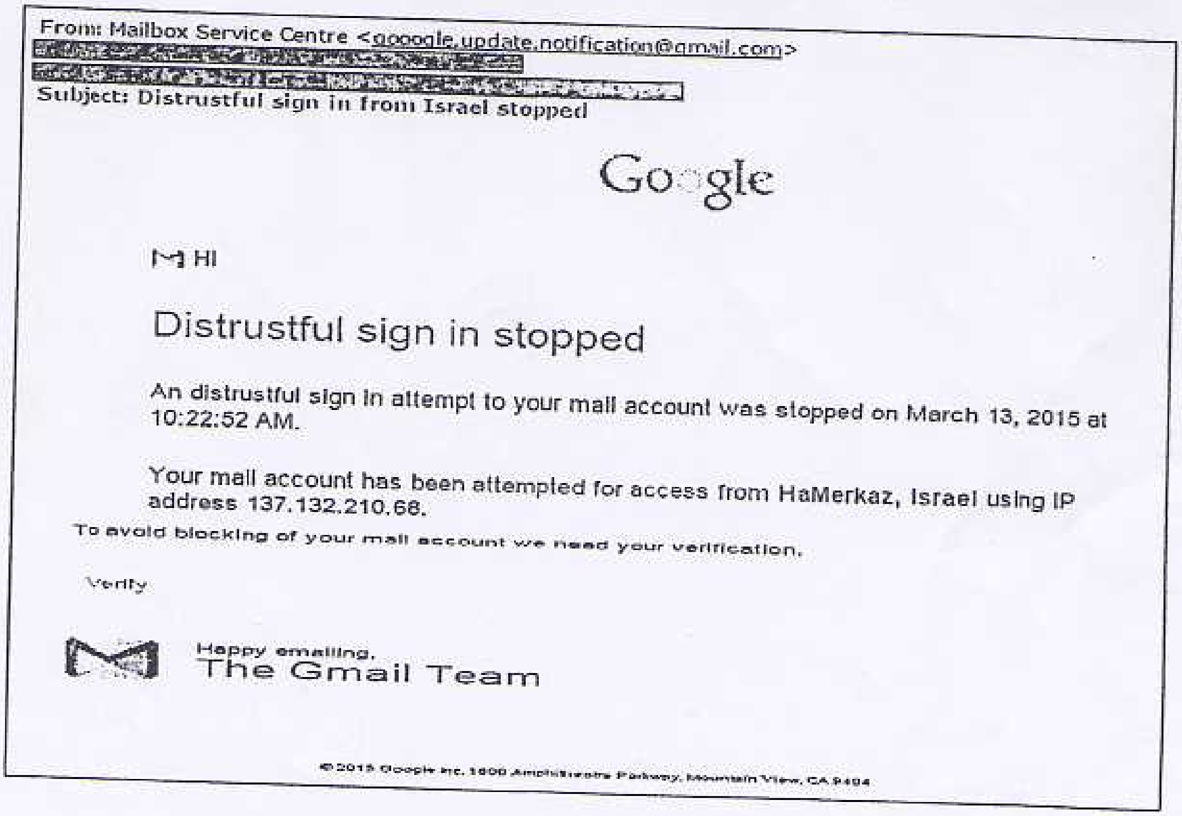
Click Here

WARNING!!! Email owner who refuses to upgrade their account within 48 hrs notification of this update will permanently be deleted from our database and can also lead to malfunctioning of the client or user's account and we will not be responsible for loosing your account

System Administrator

Anx F

Phishing (Fake Email) - 06



From: Mailbox Service Centre <gooogle.update.notification@gmail.com>

[redacted]

Subject: Distrustful sign in from Israel stopped

Google

HI

Distrustful sign in stopped

An distrustful sign in attempt to your mail account was stopped on March 13, 2015 at 10:22:52 AM.

Your mail account has been attempted for access from HaMerkaz, Israel using IP address 137.132.210.66.

To avoid blocking of your mail account we need your verification.

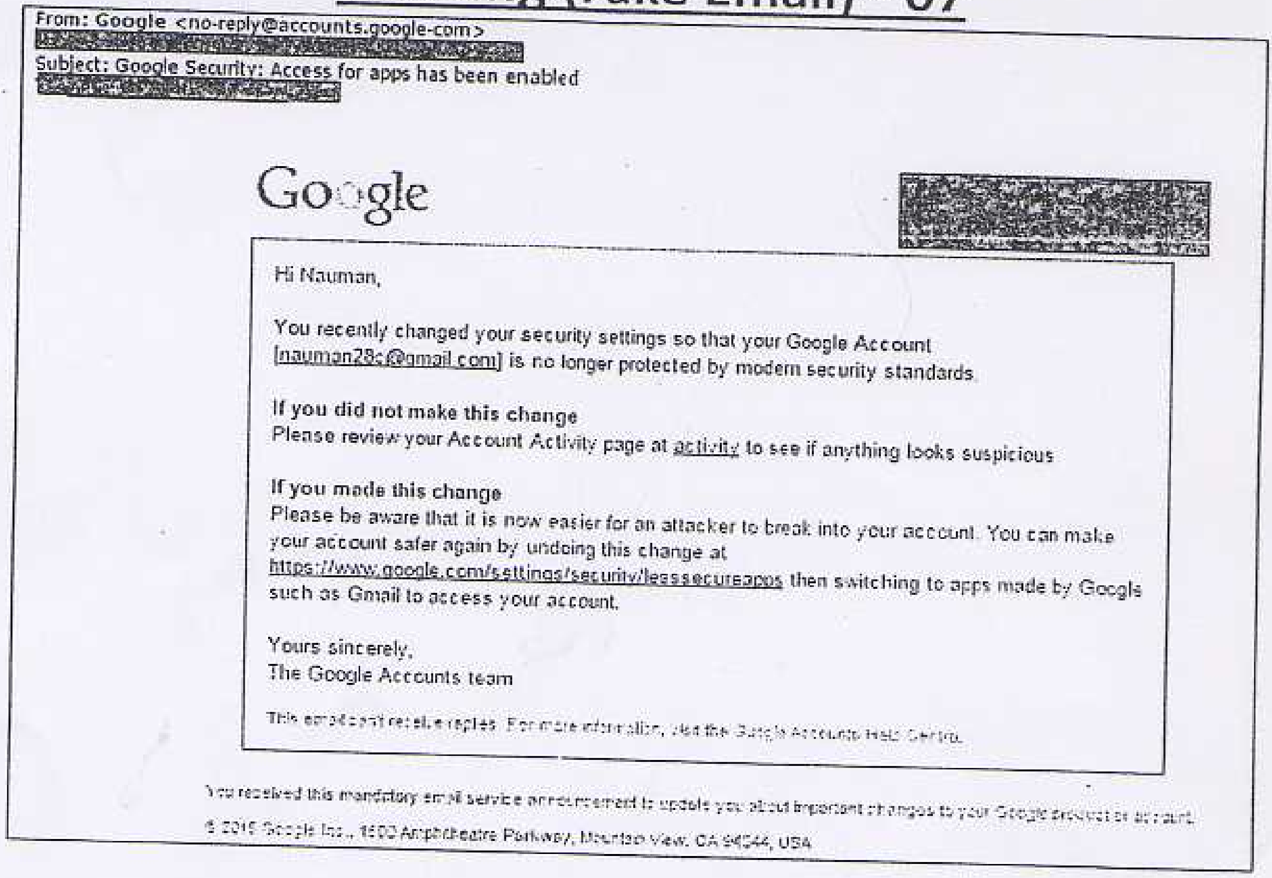
Verify

Happy emailing,
The Gmail Team

©2015 Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 9404

Anx G

Phishing (Fake Email) - 07



From: Google <no-reply@accounts.google-com>
[redacted]
Subject: Google Security: Access for apps has been enabled
[redacted]

Google

[redacted]

Hi Nauman,

You recently changed your security settings so that your Google Account [nauman28c@gmail.com] is no longer protected by modern security standards.

If you did not make this change
Please review your Account Activity page at activity to see if anything looks suspicious

If you made this change
Please be aware that it is now easier for an attacker to break into your account. You can make your account safer again by undoing this change at https://www.google.com/settings/security/lesssecureapps then switching to apps made by Google such as Gmail to access your account.

Yours sincerely,
The Google Accounts team

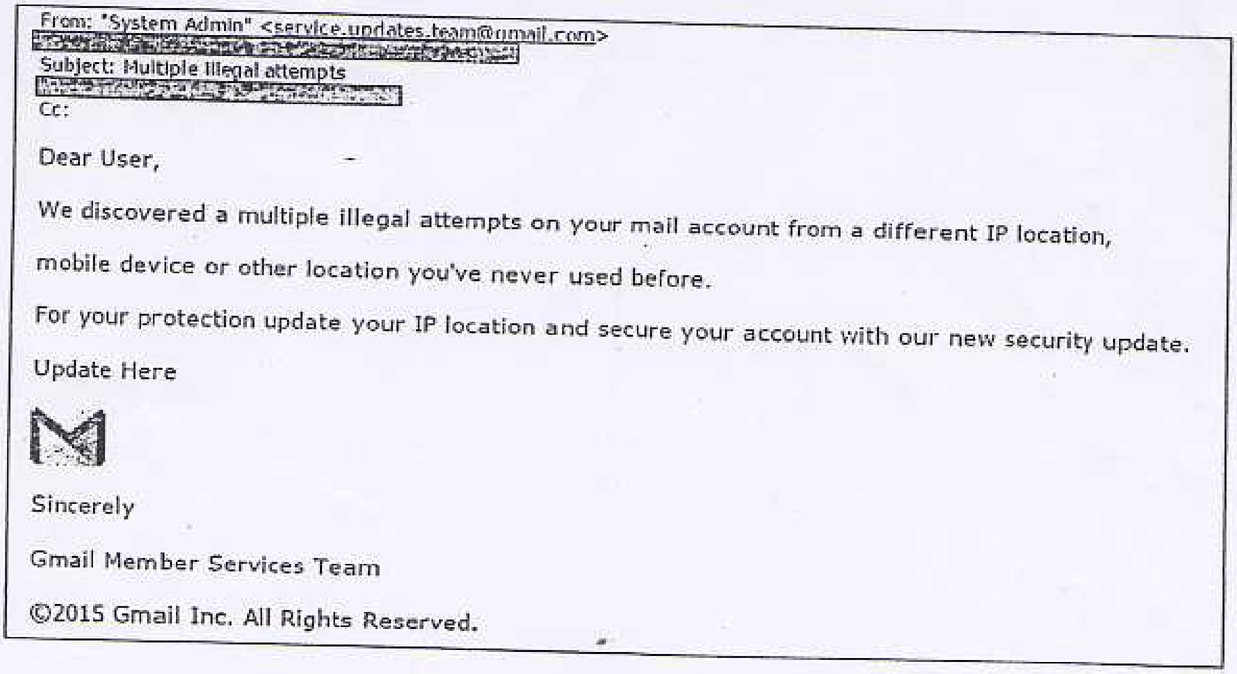
This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2015 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94044, USA

Anx H

Phishing (Fake Email) - 08



From: "System Admin" <service.updates.team@gmail.com>
[redacted]
Subject: Multiple Illegal attempts
[redacted]
Cc:

Dear User,

We discovered a multiple illegal attempts on your mail account from a different IP location, mobile device or other location you've never used before.

For your protection update your IP location and secure your account with our new security update.

Update Here

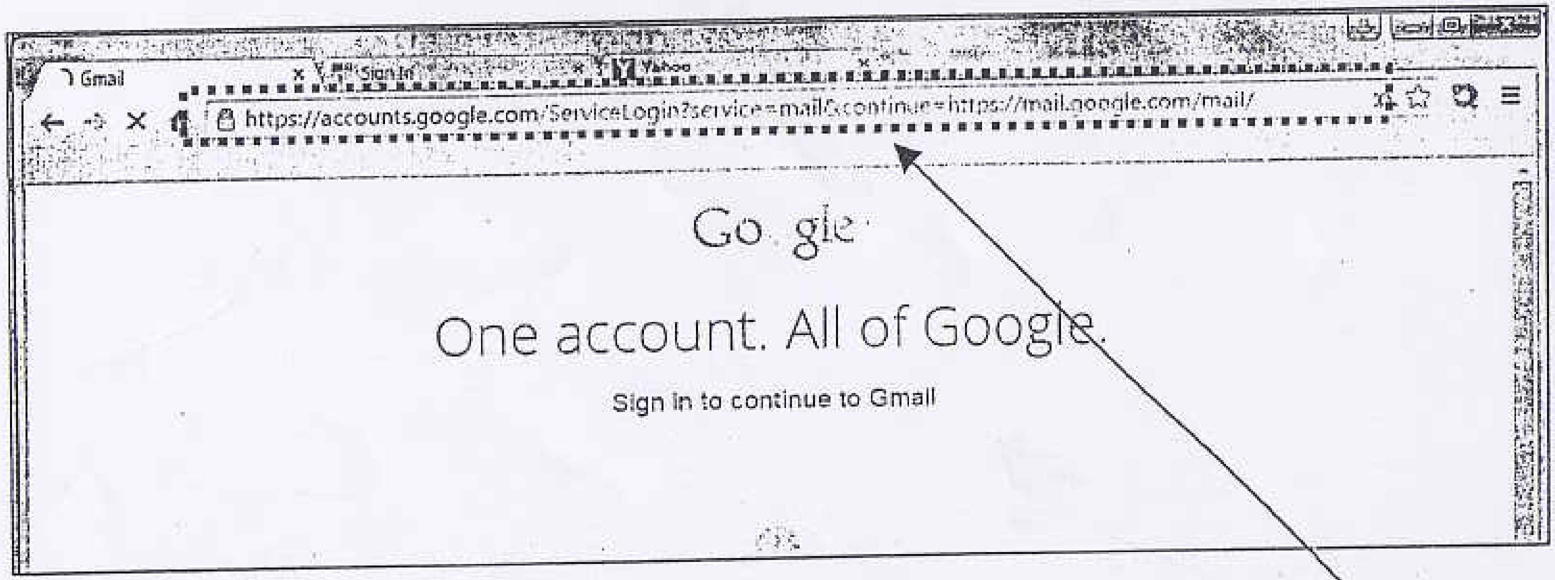
Sincerely

Gmail Member Services Team

©2015 Gmail Inc. All Rights Reserved.

Anx J

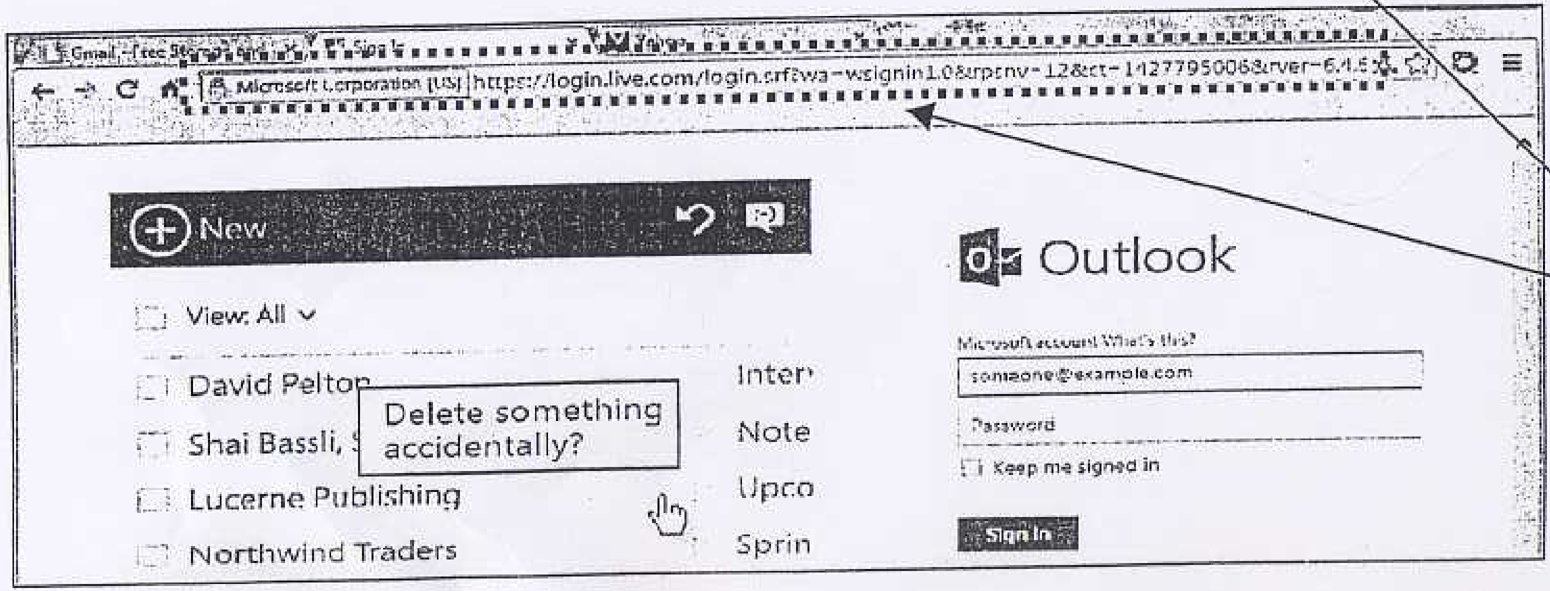
Verification of URL Before Entering Username / Password



https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/

One account. All of Google.

Sign in to continue to Gmail



https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=12&ct=1427795006&rver=6.4.6

David Pelton

Shai Bassli,

Lucerne Publishing

Northwind Traders

Delete something accidentally?

Microsoft account What's this?

someone@example.com

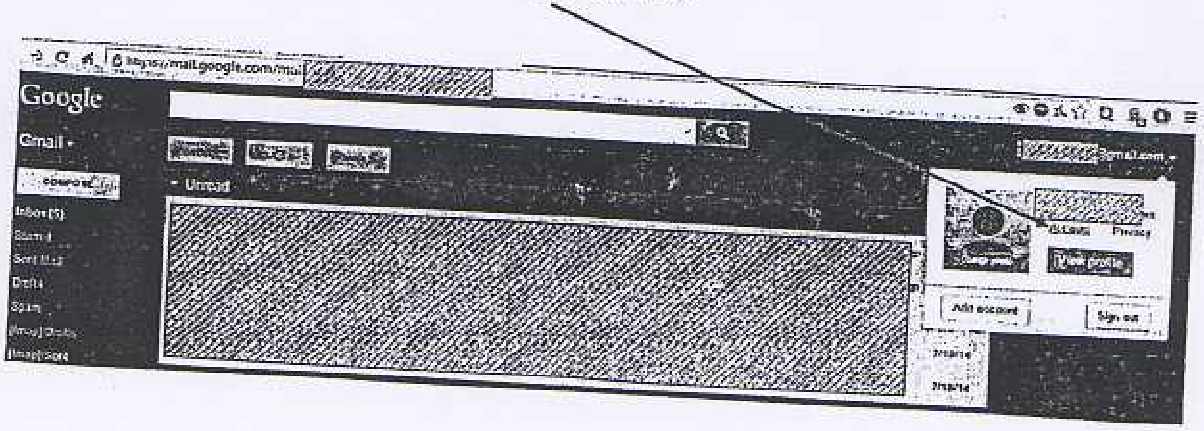
Password

□ Keep me signed in

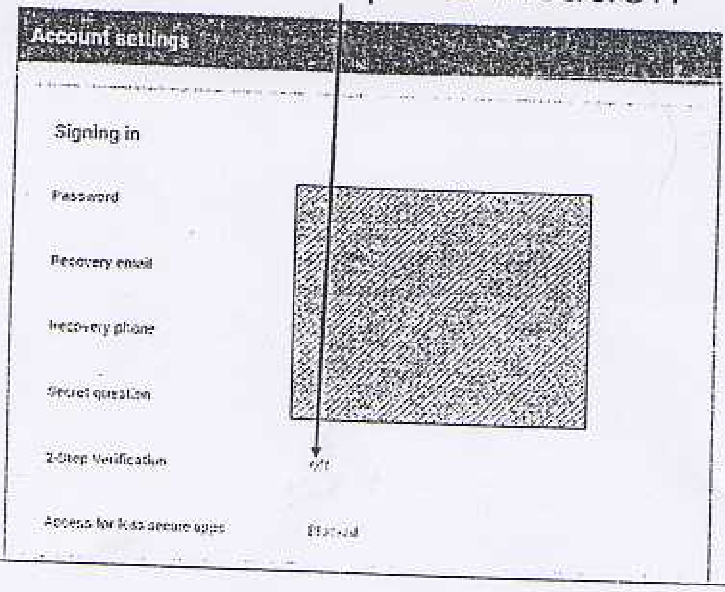
Verify URL in Address Bar

Enabling two factor authentication in gmail

Step 1 – Click on "Accounts"



Step 2 – Click on 2-Step Verification



Account settings

Signing in

Password

Recovery email

Recovery phone

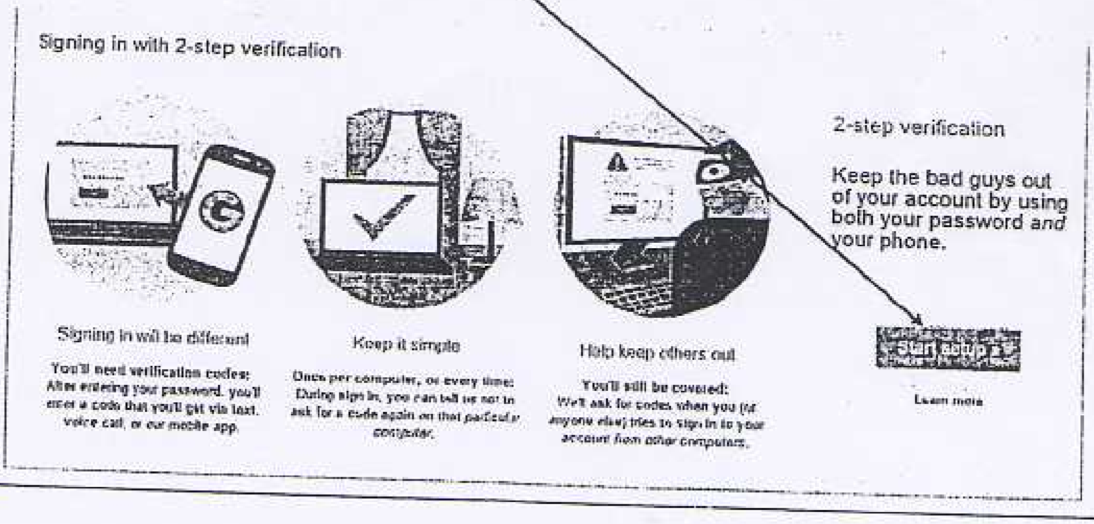
Secret question

[redacted]

2-Step Verification Off

Access for less secure apps Enabled

Step 3 – Click Start Setup



Signing in with 2-step verification

Signing in will be different

You'll need verification codes: After entering your password, you'll enter a code that you'll get via text, voice call, or our mobile app.

Keep it simple

Once per computer, or every time: During sign in, you can tell us not to ask for a code again on that *particular computer.*

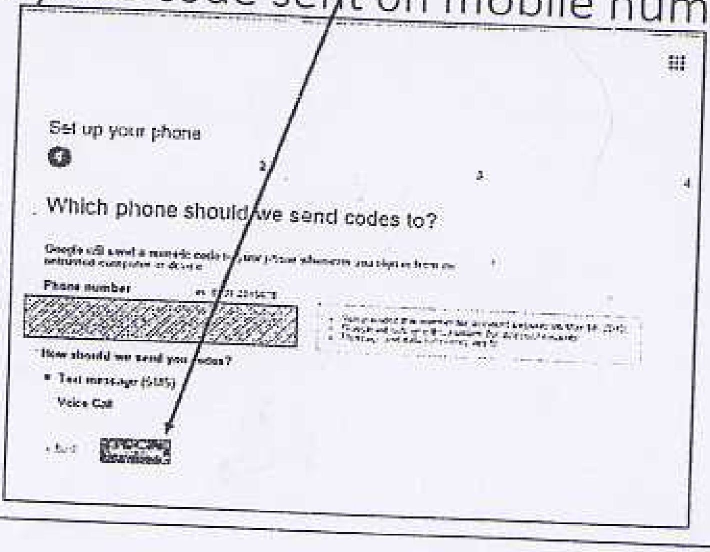
Help keep others out

You'll still be covered: We'll ask for codes when you (or anyone else) tries to sign in to your account from other computers.

2-step verification

Keep the bad guys out of your account by using both your password *and* your phone.

Step 4 – Enter password again and start setting phone number and click Send Code. IN next screen, verify the code sent on mobile number



Set up your phone

Which phone should we send codes to?

Google will send a numeric code to your phone whenever you sign in from an untrusted computer or device

Phone number [illegible]

[redacted]

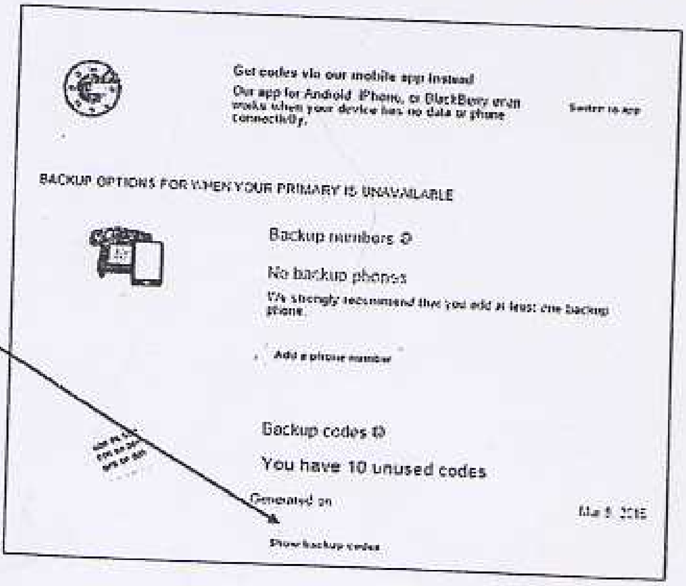
How should we send you codes?

- Text message (SMS)
- Voice Call

Steps till here will enable you to sign in using a code which is sent from google to your mobile number, each time you sign in

Step 5 – You can print a set of 10 codes. This will enable 2-factor authentication using one code which cant be used next time. You will not be dependent on mobile phone.

Keep these codes safe and generate new codes before they are finished



Get codes via our mobile app instead

Our app for Android, iPhone, or BlackBerry even works when your device has no data or phone connectivity.

Switch to app

BACKUP OPTIONS FOR WHEN YOUR PRIMARY IS UNAVAILABLE

Backup numbers

No backup phones

We strongly recommend that you add at least one backup phone.

Add a phone number

Backup codes

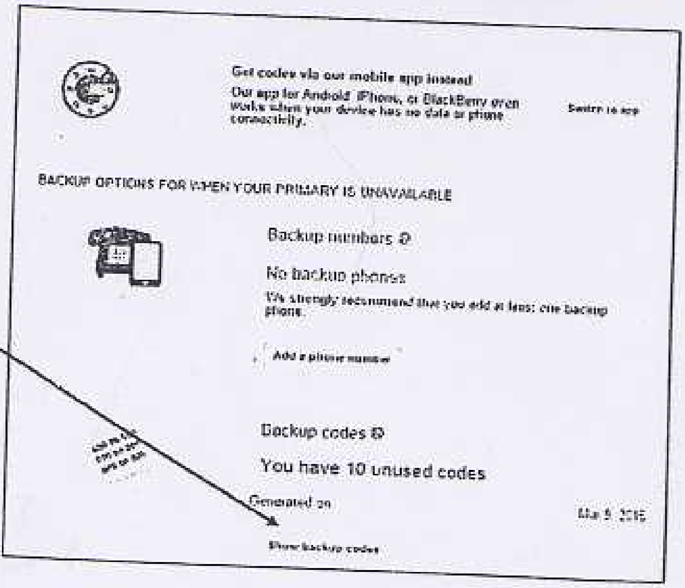
You have 10 unused codes

Generated on Mar 5, 2015

Show backup codes

Step 5 – You can print a set of 10 codes. This will enable 2-factor authentication using one code which cant be used next time. You will not be dependent on mobile phone.

Keep these codes safe and generate new codes before they are finished



Get codes via our mobile app instead

Our app for Android, iPhone, or BlackBerry even works when your device has no data or phone connectivity.

Switch to app

BACKUP OPTIONS FOR WHEN YOUR PRIMARY IS UNAVAILABLE

Backup numbers ⚙

No backup phones

We strongly recommend that you add at least one backup phone.

Add a phone number

Backup codes ⚙

You have 10 unused codes

Generated on Mar 5, 2015

Show backup codes