



Republic of the Philippines  
NATIONAL POLICE COMMISSION  
PHILIPPINE NATIONAL POLICE  
INFORMATION TECHNOLOGY MANAGEMENT SERVICE  
Camp Crame, Quezon City



**MEMORANDUM**

FOR : See Distribution  
FROM : D, ITMS  
SUBJECT : **Computer Security Threat Advisory: Upgrade Alert Modus**  
DATE : May 15, 2017

---

1. References:

- a. Attached Email received from John Mark T. Lozano; GovMail Support Team, DICT on May 8, 2017 1:46 PM;
- b. Computer Security Bulletin CSB17-001 Phishing Attempt Threat Advisory: "Mailbox Quota Exceeded" at [www.itms.pnp.gov.ph](http://www.itms.pnp.gov.ph); and
- c. Republic Act 10175 "Cybercrime Prevention Act of 2012" Chapter 2, Section 4a, 3 and 4.

2. This pertains to a recent phishing attack that attempts to draw the attention of recipients with the subject line "Upgrade Alert" while the sender may appear to be ICT DEPT <[gcassius@gosl.gov.lc](mailto:gcassius@gosl.gov.lc)>. Accordingly, the recipient will be advised to click a link to update Zimbra webmail and directed to a fake website and asked to enter private information.

3. In this regard, all PNP personnel especially those who are using e-mail in work-related activities are advise to validate first the emails received to avoid possible breaches. Also, once a message is received with same description, immediately close the message, report it as a spam and inform ITMS for awareness to other PNP offices thru the following:

- a. Telephone Number: **(02) 7230401 local 4225**;
- b. E-mail address: **[wscsditms@pnp.gov.ph](mailto:wscsditms@pnp.gov.ph)**; and
- c. Chat Service: **[www.itms.pnp.gov.ph](http://www.itms.pnp.gov.ph)**.

4. For guidance and widest dissemination.

**EDWIN JOSE G NEMENZO**  
Police Chief Superintendent

**Distribution:**

Command Group  
D-Staff  
P-Staff  
D, NSUs  
RD, PROs

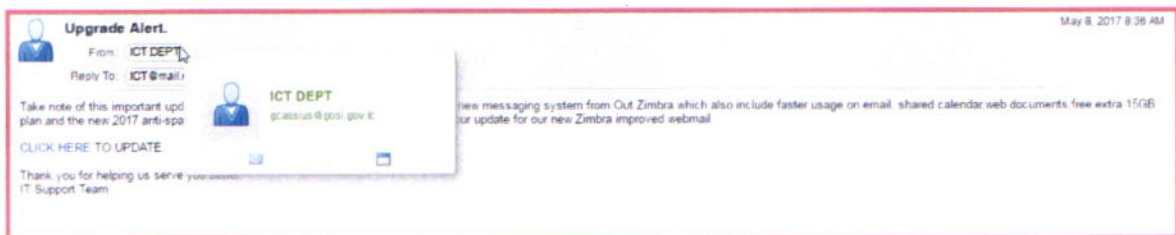
**From:** "GovMail Support" <johnmark.lozano@dict.gov.ph>  
**To:** "agencyadmins" <agencyadmins@liham.gov.ph>  
**Cc:** "GovMail Support" <govmailsupport@dict.gov.ph>  
**Sent:** Monday, May 8, 2017 1:46:19 PM  
**Subject:** Phishing Attempt Threat Advisory: "Upgrade Alert."

Good day!

Dear GovMail Admins,

Phishing is a fraudulent process used by spammers to acquire sensitive information from users such as usernames, passwords, and credit card details. Email recipients are often deceived by phishing attempts since messages appear to be sent by legitimate and trustworthy sources.

In recent days, we've learned of a new phishing attack that attempts to draw the attention of recipients with the subject line "Upgrade Alert.", while the sender may appear to be "ICT DEPT" <gcassius@gosl.gov.lc>".



Users are directed to a fake website and asked to enter private information.

In the event that you receive a message fitting this description, close the message immediately and report it as spam.

Our email traffic is filtered by our anti-spam and antivirus service, which provides you with protection against dangerous viruses and spam.

However, some spam may occasionally get through to your inbox or be diverted to your Junk folder, so please be cautious.

For issues and concerns, please create an account and ticket under **Helpdesk** queue at the **iGovPhil Helpdesk**

or email us at [govmailsupport@dict.gov.ph](mailto:govmailsupport@dict.gov.ph) or [helpdesk@i.gov.ph](mailto:helpdesk@i.gov.ph)

Respectfully yours,

**John Mark T. Lozano**

GovMail Support Team

Department of Information and Communications Technology

ICT Office Bldg., C.P. Garcia Avenue, Diliman, Quezon City

Tel. No. +63 2 920-0101 loc. 2703

Email: [govmailsupport@dict.gov.ph](mailto:govmailsupport@dict.gov.ph)

<https://www.dict.gov.ph>

Standard Disclaimer:

The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and other parties authorized to receive it. It may contain confidential or legally privileged communication. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this e-mail and then immediately delete it from your system. Opinions contained in this e-mail or any of its attachments do not necessarily reflect the opinions of the Department of Information and Communications Technology.