☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt ☐ Mark Subject Restricted

Update on Government-wide Phishing Drill Campaign
Administrator EDB

14/06/2019 15:32

From: Administrator EDB/EDB/HKSARG
To:
Bcc:
Sent by: Carrie KL WONG/EDB/HKSARG

History: This message has been forwarded.

[This email is sent to all EDB staff (Office) for attention.]

Dear all,

Update on Government-wide Phishing Drill Campaign

I refer to the preceding notification about the Government-wide Phishing Drill Campaign and the updates from the OGCIO attached below. As informed by the OGCIO on 6.6.2019, in response to feedback received from B/Ds, the Phishing Drill Programme Office has enhanced their system to record the email addresses of users who have clicked on pseudo-phishing links, and they will provide such information to the Departmental IT Security Officer (DITSO) of the respective B/D by monthly reports. The purpose of the change is to allow for easier follow-up with the concerned users about the proper handling of emails.

2. The phishing drill for EDB users, with the mentioned enhancements, would start in mid June 2019.

3. For enquiries, please contact OS Help Desk at 3509 8494 (Tamar CGO) or 3540 7305 (Wu Chung House). For VIP Users, please contact VIP Support Team at 3509 8492 (Tamar CGO) or 3540 7338 (Wu Chung House).

EDB Administrator

OGCIO Phishing Drill Programme Office | Dear DITSOs, Thank... | 06/06/2019 10:42:40 AM

From: OGCIO Phishing Drill Programme Office/OGCIO/HKSARG@OGCIO
To: OGCIO Phishing Drill Programme Office/OGCIO/HKSARG@OGCIO
Date: 06/06/2019 10:42 AM
Subject: Updates on Government-wide phishing drill campaign

Dear DITSOs,

Thank you very much for your assistance and support in the Government Wide Phishing Drill Campaign. The first round of the campaign commenced in end May 2019 starting with sending pseudo-phishing emails to some B/Ds.

2. Since then, the Programme Office has received suggestions from B/Ds requesting for more information on user clicks for their easy follow-up, such as who have clicked the pseudo-phishing links, who have provided further information upon request by the pseudo-phishing emails.

Enhanced Arrangement

3. With such information, B/Ds can better master the situation and make necessary follow up actions including arranging appropriate training in raising their staff's awareness in handling phishing email. Hence, the Programme Office has enhanced the system and will provide an enhanced set of month-end phishing drill reports to individual DITSOs for necessary follow-up:

- Statistics of pseudo-phishing links clicked by phishing types of the respective B/D
- Statistics of pseudo-phishing links clicked by phishing types of all B/Ds
- List of email addresses of users having clicked on pseudo-phishing links with phishing types of the respective B/D

4. A suite of seven 2-minute training videos has been produced and a series of seminars would be organised by the Programme Office for users to view and participate. In addition, video streams of the past seminars on prevention of phishing email organised by OGCIO are hosted under CSTDI CLC Plus for users to view.

Suggested follow-up actions

5. Based on the drill reports provided, B/Ds should take necessary actions to promote awareness, down to individual users as appropriate. The actions include the following:

- Advise users to observe the Practice Guide on the Use of Electronic Mail (e-mail), in particular Section 3.3 - Handling of Incoming E-mails
  (https://itginfo.ccgo.hksarg/content/imx/email_practice_guide.asp)

- Advise users to view the training videos in the thematic website of the Campaign
  (https://itginfo.ccgo.hksarg/content/phishing_training/)

- Encourage users to participate in the cyber security seminars organised by OGCIO and CSTDI, or join cyber security seminars organised by your own department.

- Advise users to view the video streams of the past seminars on prevention of phishing email hosted under CSTDI CLC Plus
  (https://www.clcplus.cstdi.gov.hk/clcplus/portal/deptResources/226)

Contact us

6. We stand ready to support B/Ds to raise user awareness of phishing and the capability in defending against phishing attacks. Meanwhile if you have any suggestions on pseudo phishing templates, please feel free to share with us. If you have any questions, please contact us at Notes email: OGCIO Phishing Drill Programme Office/OGCIO/HKSARG; or Tel: 3182 6532.

Best Regards,
OGCIO Phishing Drill Programme Office

Distribution of this e-mail:
- DITSOs

c.c.
- eBCs
- Phishing Drill Coordinators

Administrator EDB [This email is sent to all EDB staff (Office) for... 27/05/2019 09:54:36 AM

From: Administrator EDB/EDB/HKSARG
To:
Date: 27/05/2019 09:54 AM
Subject: Notification about the Government-wide Phishing Drill Campaign
Sent by: Carrie KL WONG

[This email is sent to all EDB staff (Office) for attention.]

Dear all,

Notification about the Government-wide Phishing Drill Campaign

Nowadays, more than 90% of hacking attacks start with phishing emails, which are deceptive emails from senders disguising as trustworthy entities (e.g. banks, online service providers). Phishing emails attempt to obtain sensitive information, such as user names, passwords and credit card details from the targeted recipients. Some phishing emails also trick users into downloading malicious software (e.g. ransomware or backdoors) to carry out further attacks.

2. As a central initiative to raise government users' awareness of phishing and their capability in defending against phishing attacks, the Office of the Government Chief Information Officer (OGCIO) has organised the Government-wide Phishing Drill Campaign commencing May 2019 for around 12 months covering **all government users with official Internet email accounts**.

3. The Campaign comprises training videos, quizzes and phishing drill. **The phishing drill for EDB users would be conducted from June 2019 to April 2020. During this period, EDB users with official Internet email accounts (e.g. userA@edb.gov.hk) would receive a number of harmless pseudo-phishing emails, which are similar to the real phishing emails.** To simulate real-world practice, users would not be informed of the exact schedules and contents of the phishing drill. ~~The phishing drill will not identify individual users who have clicked on the embedded files or links in the pseudo-phishing emails.~~ Users who have clicked on the embedded files or links in the pseudo-phishing emails will be automatically diverted to OGCIO's campaign website advising the proper ways of handling phishing emails.

4. Although the pseudo-phishing emails of this Campaign are harmless and will not contain any malicious contents, **please DO NOT open attachments or links in any suspicious emails as those could be REAL phishing emails containing malicious contents.**

5. Users are encouraged to visit the thematic website of the Campaign, with education resources, to enhance your knowledge and capability in defending against phishing attacks:

https://itginfo.ccgo.hksarg/content/pdc/

6. Taking this opportunity, we would like to remind users that information security is the responsibility of every staff member in the Government. Users should NOT open any suspicious emails, attachments and hyperlinks, no matter the email is from Lotus Notes or your private email account. Spam emails should be ignored or deleted. Please beware that phishing emails could lead to malware infection (e.g. ransomware) or even security breach.

7. For further enquiries, please contact OS Help Desk at 3509 8494 (Tamar CGO) or 3540 7305 (Wu Chung House). For VIP Users, please contact VIP Support Team at 3509 8492 (Tamar CGO) or 3540 7338 (Wu Chung House).

EDB Administrator