Headers

Date: `Sun, 12 May 2024 04:10:52 +0000`
Subject: `Reset your Dropbox password`

To: `emily[.]nguyen@glbllogistics[.]co`
From: `no-reply@dropbox[.]com`

Reply-To: `N/A`
Return-Path: `0101018f6aff12b2-5bcaa145-861b-45da-a06e-b5c1ee3ca941-000000@email.dropbox.com`

Message-ID: `0101018f6aff12b2-5bcaa145-861b-45da-a06e-b5c1ee3ca941-000000@us-west-2.amazonses.com`

URLs

- `hxxps[://]www[.]dropbox[.]com/l/ABCIzswwTTJ9--CxR05fYXX35pPA-Y0m3PY/forgot_finish`
- `hxxps[://]www[.]dropbox[.]com/l/AADQ493u2QLcZrv2kCW6C6i0Ac-mR0hUXxU/help/365`
- `hxxp[://]www[.]w=3[.]org/TR/REC-html40/loose[.]dtd`
- `hxxp[://]www[.]w3[.]org/1999/xhtml`
- `hxxp[://]fonts[.]googleapis[.]com/css?f=amily=3DOpen+Sans`
- `hxxps[://]www[.]dro=pbox[.]com/l/AADiZXaA7dm2EyafvAILlHJAzwU3D55FQwg/forgot_finish`

Attachments

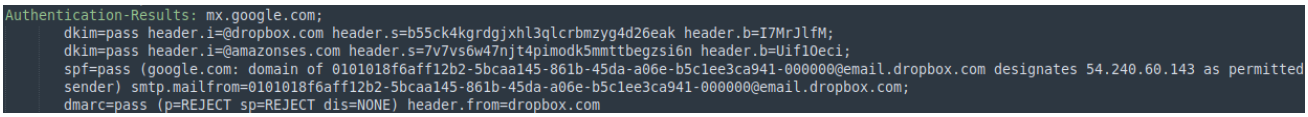
No Attachments were found in the email.

Description

Emily Nguyen, a member of the marketing team, recently had trouble signing into her Dropbox account after trying to access it for the first time in months and reached out to her manager for assistance. The next day, she received an email that claims a password change request was made for her Dropbox account. The email includes a link for resetting her password, but Emily is unsure if the request is legitimate. Concerned about potential phishing, she has forwarded the email to the security team for analysis.

DMARC/SPF/DKIM

- The email passed all SPF, DMARC, and DKIM checks



Sender Analysis

- Talos Intelligence reports a **favorable** reputation rating for `no-reply@dropbox[.]com`
- Talos Intelligence also reports a **favorable** rating for the return -path: `0101018f6aff12b2-5bcaa145-861b-45da-a06e-b5c1ee3ca941-000000@email.dropbox.com`
- No other return sender or alternate **reply to** field found.
- Preliminary investigation suggests no IOC or malicious behavior from sender details.

URL Analysis

- Performed investigation on the website: `hxxps[://]www[.]dropbox[.]com/l/AADQ493u2QLcZrv2kCW6C6i0Ac-mR0hUXxU/help/365`
  - Talos Intelligence gave a **Favorable Reputation**
  - virus total also had a clean response with **no venders flagging** as malicious
  - phish tank **found no malicious indicators**
  - **No malicious** behavior found on urlscan.io
  - Urlvoid found **no malicious reputation indicators**
- Performed investigation on the website: `https://www.dropbox.com/l/AACK_ihQPkvHRxrdwgoAKiptOg-dtAhzX2Y`
  - Talos Intelligence gave a **Favorable Reputation**

    - virus total also had a clean response with **no venders flagging** as malicious
    - phish tank **found no malicious indicators**
    - **No malicious** behavior found on urlscan.io
    - Urlvoid found **no malicious reputation indicators**
- Performed investigation on the website: `hxxps[://]www[.]dropbox[.]com/l/ABCIzswwTTJ9--CxR05fYXX35pPA-Y0m3PY/forgot_finish`
    - Talos Intelligence gave a **Favorable Reputation**
    - virus total also had a clean response with **no venders flagging** as malicious
    - phish tank **found no malicious indicators**
    - **No malicious** behavior found on urlscan.io
    - Urlvoid found **no malicious reputation indicators**
- Performed investigation on the website: `hxxps[://]www[.]dropbox[.]com/l/AAAN2hEjsnK4UD1fkJxpXCS15vzTRW64Tjc/help/365`
    - Talos Intelligence gave a **Favorable Reputation**
    - virus total also had a clean response with **no venders flagging** as malicious
    - phish tank **found no malicious indicators**
    - **No malicious** behavior found on urlscan.io
    - Urlvoid found **no malicious reputation indicators**
- Reputational checks determined that no malicious behavior has been detected in the drobox URLs.

Verdict

- After investigating the sender and URLs embedded in the email, it is highly likely that the email is not a phishing attempt, and is a legitimate request for password verification. No URLs were found to behave suspiciously or have failed reputation checks. No attachments or obfuscation behavior was detected anywhere in the email or structure.

Defensive Actions

- No defensive actions are necessary, the email is likely not a phishing attempt. However, for an extra layer of security, the user is advised to reset their account through the official dropbox website portal and not the link. A splunk or SIEM rule to capture and monitor further

dropbox emails may be useful, especially if more than one employee receives similar phishing emails.