Workgroup:	Internet Engineering Task Force
Internet-Draft:	draft-vgpastor-email-phishing-training-00
Published:	2 April 2024
Intended Status:	Informational
Expires:	4 October 2024
Author:	V. G. P. vgpastor, Ed.

Proposal for the Introduction of Email Headers for Phishing Detection Training

Abstract

This document proposes the addition of new email headers designed specifically to identify emails that are sent as part of phishing detection training programs. These headers would allow recipients to verify the authenticity of training emails using DNS queries to confirm that the sending domains are authorized to send these types of emails.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 October 2024.

Copyright Notice

Table of Contents

1. Introduction

Phishing remains one of the most significant security threats on the Internet today. Training users to detect phishing attempts is a crucial tool in defending against these types of attacks. However, the effectiveness of these training programs can be compromised if emails used for training are incorrectly flagged and filtered by anti-phishing solutions.

This paper proposes a solution to this problem by introducing specific headers in training emails that would allow email systems to correctly identify them and prevent their filtering, while also providing a verification mechanism to confirm the legitimacy of these emails. .

1.1. Goals

The main objective of this proposal is to improve the effectiveness of phishing detection training programs by introducing a mechanism that allows email systems to identify and authenticate training emails, maintaining security in email systems and avoiding abuse of this mechanism.

The main motivation behind this proposal is to improve the effectiveness of phishing detection training programs. Currently, emails used in these programs can be incorrectly flagged as phishing attempts by anti-phishing solutions, which can lead to users not receiving proper training or the emails being filtered before they can be used for training.

Finally, it is very important that users can use phishing detection reporting systems to improve the use of these systems, as well as train users themselves in the detection and prevention of this type of attacks. These reports must be able to discard phishing detection training emails so as not to generate false positives, as well as be able to forward said emails to phishing detection training providers so they can be analyzed and improved.

1.2. Description of the Proposal

The proposal consists of the following main elements, addition of email headers, sender legitimation and link validation mechanism.

1.2.1. Adding Email Headers

The proposal includes the introduction of new email headers for phishing detection training emails: - Phishing-Simulation: Mandatory | A unique identifier for the training session. It can be shared between multiple recipients, but cannot be repeated for the same recipient. - Phishing-Simulation-Provider: Required | The domain of the phishing detection training provider. - Phishing-Simulation-Auth: Required | DNS record that contains the email authentication information. - Phishing-Simulation-Report: Optional | A link or email to report phishing detection training emails.

1.2.1.1. Phishing-Simulation Header

Unique identifier for the training session. This identifier allows identification of the email as a phishing simulation and allows email systems to perform DNS queries to verify the authenticity of the email. At a training level it can be used to measure the effectiveness of specific phishing detection training.

```
Phishing-Simulation: unic-identifier
```

1.2.1.2. Phishing-Simulation-Provider Header

Identification of the phishing detection training provider. This field allows email systems to identify the domain of the training provider and use it to verify the authenticity of the email. The same company may have several phishing detection training providers, so it is important that this header be mandatory.

By using user phishing detection reporting systems, you can identify which phishing detection training providers are being most effective and those who need improvement. Finally you can use these rules to filter reported messages.

`Phishing-Simulation-Provider: example.com`

1.2.1.3. Phishing-Simulation-Auth Header

DNS record that contains the email authentication information. This record must be dynamic for each domain since it allows you to publicly hide whether a domain uses this type of phishing detection training.

`Phishing-Simulation-Auth: xxxxxxxxxxx`

1.2.1.4. Phishing-Simulation-Report Header

Email address or url endpoint where to send the reported email through a PUT request. It is important that the original headers of the email be sent to the mailbox or url endpoint for analysis, also allowing their analysis. `Phishing-Simulation-Report: reports@example.com`

1.2.2. DNS Verification Mechanism

Details how mail systems can use the proposed headers to perform DNS queries and verify the authenticity of training emails.

The domain owner must add a TXT record in their DNS with the following format: The DNS record should be dynamic for each domain, this way it can be hidden if a domain uses this type of phishing detection training.

The content of the registry stores both the emails authorized to send the emails and the domains authorized for the links.

`xxxxxxxxxxx.example.com TXT v:pdt1; sender:domain-that-send-email.com,domain-that-send-email2.com ;links:domain-links.com,domain-links.com`

It is also necessary that the values can be authorized externally, in case a provider needs to modify, add or delete domains for both sending and links, clients do not have to continually modify their own records.

Provider DNS entry `_pdt.example.com TXT v:pdt1; sender:domain-that-send-email.com,domain-that-send-email2.com ;links:domain-links.com,domain-links2.com`

Client DNS entry `xxxxxxxxxxx.example.net TXT v:pdt1; sender:domain-that-send-email3.com,_pdt.example.com ;links:domain-links3.com,_pdt.example.com`

1.2.3. Link Validation Mechanism

Validating links within the email is an important step in preventing users from clicking on malicious links. The addition of a link validation mechanism is proposed to allow email systems to verify the authenticity of links in training emails.

It must be verified that all the links contained in the body of the email are within those enabled in the DNS record of the sender's domain.

1.2.4. Email Report

When the end user receives a phishing training email that is identified by the user as such, the user may use the usual means for reporting this email.

The mail provider, or the email client, when the header in the email `Phishing-Simulation-Report` exists, may send the email to the email address or link provided in the header so that the detection training provider of phishing can analyze the email and improve its training, it is important that this report includes the original headers of the email for analysis.

1.3. Implementation

1. Phishing detection training providers should implement the proposed email headers in their training emails.
2. Phishing detection training providers must legitimize their authorized domains for both sending emails and links to avoid abuse of this mechanism.
3. Customers must configure their DNS records with the necessary values to allow verification of training emails.
4. The email system upon receiving a phishing detection training email must perform a DNS query to verify the authenticity of the email and the links contained in the email.
    1. If the DNS query is successful, the email continues verification.
    2. It checks if the sender's domain is authorized to send phishing detection training emails.
    3. It is checked if the links contained in the email are authorized to be used in phishing detection training emails.
    4. If the verification is successful, the email is delivered to the recipient. If any of the previous steps fail, the email should be marked as suspicious.
5. Users should use phishing detection reporting systems to report suspicious emails and improve the effectiveness of phishing detection training programs.
    1. The email system will send the reported email to the phishing detection training provider for analysis and improvement.
    2. If there is no entry for the report, the sending of the email to anti-phishing systems will be stopped and it will be marked as suspicious.

1.3.1. Implementation in email sending provider

When a client of an email sending provider, such as Sendgrid, Mailgun, etc., sends a phishing detection training email, the provider can verify if they are authorized to send this type of email to ensure proper use of the email. their systems. 1. The recipient of the phishing detection training email must have a DNS record with allowed origin information. 2. The email sending provider must perform a DNS query to verify the authenticity of the email and the legitimacy of the sender to send these emails to the recipient.

1.4. Example

- example.com -> Phishing detection training provider domain
- example.net -> Domain of the client that receives the phishing detection training email
- test.com -> Domain used to send the phishing detection training email
- example.org -> Domain used for links in the phishing detection training email

1.4.1. DNS entries

```
_pdt.example.com TXT v:pdt1; sender:test.com ;links:example.org
```

```
2654896524568._pdt.example.net TXT v:pdt1; sender:_pdt.example.com
;links:_pdt.example.com
```

1.4.2. E-Mail sent

``` From: fake@mail.test.com To: user@example.net Subject: Message from CEO Message-ID: 05c18622-f2ad-cb77-2ce9-a0bbfc7d7ad0@example.com Date: Mon, 25 Mar 2024 10:00:00 -0400 Phishing-Simulation: fcbdc611-3807-4cfc-a521-f7beb4ca39ff Phishing-Simulation-Provider: example.com Phishing-Simulation-Auth: 2654896524568 Phishing-Simulation-Report: reports@example.com Content-Type: text/plain; charset=utf-8

Please send 1M USD to the following account: https://transfers.example.org/bank-account

Regards ```

## 2. Security

The security implications of this proposal have been considered and recommendations have been provided to mitigate potential risks.

Currently, no significant safety risks associated with this proposal have been identified. However, it is important that senders of training emails follow the security recommendations provided in this document to prevent abuse of this mechanism.

This proposal does not take into account the enablement of sending emails to particular end users who use generic email accounts (google.com, live.com, etc.), however the email providers themselves could add this functionality to improve the security of its users, allowing each user to enable a phishing detection training provider.

## 3. IANA Considerations

This document includes requests to IANA to register the proposed new email headers.
```

Acknowledgements

Special thanks to Zepo.app for the inspiration for the creation of this document and to all of you who have helped me review and improve this document.

Contributors

Zepo.app
Email: info@zepo.app
URI: https://zepo.app

Inspiration for the creation of this document.

Author's Address

Victor Garcia Pastor (EDITOR)
Email: vgpastor08@gmail.com
URI: https://twitter.com/vgpastor