Internet Engineering Task Force (IETF)
Request for Comments: 8058
Category: Standards Track
ISSN: 2070-1721

J. Levine
Taughannock Networks
T. Herkula
optivo GmbH

January 2017

Signaling One-Click Functionality for List Email Headers

Abstract

This document describes a method for signaling a one-click function for the List-Unsubscribe email header field. The need for this arises out of the actuality that mail software sometimes fetches URLs in mail header fields, and thereby accidentally triggers unsubscriptions in the case of the List-Unsubscribe header field.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8058.

Table of Contents

1. Introduction and Motivation

A List-Unsubscribe email header field [RFC2369] can contain HTTPS [RFC7230] URIs. In that header field, the HTTPS URI is intended to unsubscribe the recipient of the message from the list. But anti-spam software often fetches all resources in mail header fields automatically, without any action by the user, and there is no mechanical way for a sender to tell whether a request was made automatically by anti-spam software or manually requested by a user. To prevent accidental unsubscriptions, senders return landing pages with a confirmation step to finish the unsubscribe request. A live user would recognize and act on this confirmation step, but an automated system would not. That makes the unsubscription process more complex than a single click.

Operators of broadcast marketing lists tend to be primarily concerned about deliverability of their mail: whether the mail is delivered to the recipients and how the messages are presented, e.g., whether in the primary inbox or in a junk folder. Many mail systems allow recipients to report mail as spam or junk, and mail streams from senders whose mail is often reported as junk tend to have poor deliverability. Hence, the mailers want to make it as easy as possible for recipients to unsubscribe; if an unsubscription process is too difficult, the recipient's alternative is to report mail from the sender as junk until the mail no longer appears in the recipient's inbox.

Operators of recipient mail systems are aware that their users do not make a clear distinction between unsubscription and junk. In some cases, they allow trustworthy mailers to request notification when

their mail is reported as junk so they can unsubscribe the recipient, but the process of identifying trustworthy mailers and notifying them does not scale well to large numbers of small mailers. This specification provides a way for recipient systems to notify the mailer automatically, using only information within the mail message, and without prearrangement. Some recipient systems might wish to send an unsubscription notice to mailers whenever a user reports a message as junk, or they might offer the user the option of reporting and unsubscribing.

If a mail recipient is unsubscribing manually and the unsubscription process requires confirmation, the resulting web page is presented to the recipient who can then click the appropriate button. But when the unsubscribe action is combined with a user junk report, there is no direct user interaction with the mailer's website. Similarly, if a mail system automatically unsubscribes recipient mailboxes that have been closed or abandoned, there can be no interaction with a user who is not present. In those cases, the unsubscription process has to work without manual intervention, and in particular without requiring that software attempt to interpret the contents of a confirmation page.

This document addresses this part of the problem, with an HTTPS POST action for mail receivers. Mail senders can distinguish this action from other unsubscribe requests and handle it as a one-click unsubscription without manual intervention by the mail recipient.

This document has two goals:

- Allow email senders to signal that a List-Unsubscribe header field [RFC2369] has one-click functionality.

- Allow MUA (Mail User Agent) users to unsubscribe from mailing lists in a familiar environment and without leaving the MUA context. A receiving system can process an unsubscription request in the background without further interaction and know that it can be fully processed by the mail sender's system.

2. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when written in all capital letters.

3. Implementation

3.1. Mail Senders

A mail sender that wishes to enable one-click unsubscriptions places one List-Unsubscribe header field and one List-Unsubscribe-Post header field in the message. The List-Unsubscribe header field MUST contain one HTTPS URI. It MAY contain other non-HTTP/S URIs such as MAILTO:. The List-Unsubscribe-Post header MUST contain the single key/value pair "List-Unsubscribe=One-Click". As described below, the message MUST have a valid DomainKeys Identified Mail (DKIM) signature that covers at least the List-Unsubscribe and List-Unsubscribe-Post headers.

The URI in the List-Unsubscribe header MUST contain enough information to identify the mail recipient and the list from which the recipient is to be removed, so that the unsubscription process can complete automatically. Since there is no provision for extra POST arguments, any information about the message or recipient is encoded in the URI. In particular, one-click has no way to ask the user what address or from what list the user wishes to unsubscribe.

The POST request MUST NOT include cookies, HTTP authorization, or any other context information. The unsubscribe operation is logically unrelated to any previous web activity, and context information could inappropriately link the unsubscribe to previous activity.

The URI SHOULD include an opaque identifier or another hard-to-forge component in addition to, or instead of, the plaintext names of the list and the subscriber. The server handling the unsubscription SHOULD verify that the opaque or hard-to-forge component is valid. This will deter attacks in which a malicious party sends spam with List-Unsubscribe links for a victim list, with the intention of causing list unsubscriptions from the victim list as a side effect of users reporting the spam, or where the attacker does POSTs directly to the mail sender’s unsubscription server.

The mail sender needs to provide the infrastructure to handle POST requests to the specified URI in the List-Unsubscribe header, and to handle the unsubscribe requests that its mail will provoke.

The mail sender MUST NOT return an HTTPS redirect, since redirected POST actions have historically not worked reliably, and many browsers have turned redirected HTTP POSTs into GETs.

This document does not update [RFC2369], so the usage of List-Unsubscribe URIs other than for one-click remains unchanged.

3.2. Mail Receivers

A mail receiver can do a one-click unsubscription by performing an HTTPS POST to the HTTPS URI in the List-Unsubscribe header. It sends the key/value pair in the List-Unsubscribe-Post header as the request body.

The POST content SHOULD be sent as 'multipart/form-data' [RFC7578] or MAY be sent as 'application/x-www-form-urlencoded'. These encodings are the ones used by web browsers when sending forms. The target of the POST action is the same as the one in the GET action for a manual unsubscription, so this is intended to allow the same server code to handle both.

The mail receiver MUST NOT perform a POST on the HTTPS URI without user consent. When and how the user consent is obtained is not part of this specification.

4. Additional Requirements

The message needs at least one valid authentication identifier. In this version of the specification, the only supported identifier type is DKIM [RFC6376]. Hence, senders MUST apply at least one valid DKIM signature to the message.

The List-Unsubscribe and List-Unsubscribe-Post headers MUST be covered by the signature and included in the "h=" tag of a valid DKIM-Signature header field.

If the message does not have the required DKIM signature, the mail receiver SHOULD NOT offer a one-click unsubscribe for that message.

5. Header Syntax

The following ABNF imports fields, WSP, and CRLF from [RFC5322].

```
fields =/ list-unsubscribe-post

list-unsubscribe-post = "List-Unsubscribe-Post:" 0*1WSP postarg CRLF

postarg = "List-Unsubscribe=One-Click"
```

6. Security Considerations

The List-Unsubscribe header can contain a plaintext or encoded version of the recipient address, but that address is usually also in the To: header. This specification allows anyone with access to a

message to unsubscribe the recipient of the message, but that's typically the case with existing List-Unsubscribe, just with more steps.

A malicious mailer could send spam with content intended to provoke large numbers of unsubscriptions and with suitably crafted headers to send POST requests to servers that perhaps don't want them. But it's been possible to provoke GET requests in a similar way for a long time (and much easier, due to spam filter auto-fetches), so the chances of significantly increased annoyance seem low. The content of the List-Unsubscribe-Post header is limited to a single known key/value pair to prevent an attacker from creating malicious messages where the POST operation could simulate a user filling in an arbitrary form on a victim website.

The unsubscribe operation provides a strong hint to the mailer that the address to which the message was sent was valid, and could in principle be used as a way to test whether an email address is valid. In practice, though, there are simpler ways such as embedding image links into the HTML of a message and seeing whether the recipient fetches the images.

Since the mailer's server that receives the POST request cannot in general tell where the request is coming from, the URI SHOULD contain an opaque identifier or another hard-to-forge component to identify the list and recipient address. That can ensure that the request originated from the List-Unsubscribe and List-Unsubscribe-Post headers in a message the mailer sent. Also, the request MUST NOT include cookies or other context information to prevent the server from associating the request with previous web requests.

7. IANA Considerations

IANA has added a new entry to the "Permanent Message Header Field Names" registry.

Header field name: List-Unsubscribe-Post

Applicable protocol: mail

Status: standard

Author/Change controller: IETF

Specification document: RFC 8058

8. Examples

8.1. Simple

Header in Email

```
List-Unsubscribe: <https://example.com/unsubscribe/opaquepart>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

Resulting POST request

```
POST /unsubscribe/opaquepart HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 26

List-Unsubscribe=One-Click
```

8.2. Complex

Header in Email

```
List-Unsubscribe:
    <mailto:listrequest@example.com?subject=unsubscribe>,
    <https://example.com/unsubscribe.html?opaque=123456789>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

Resulting POST request

```
POST /unsubscribe.html?opaque=123456789 HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 26

List-Unsubscribe=One-Click
```

8.3. Complex with 'multipart/form-data'

Header in Email

```
List-Unsubscribe:
    <mailto:listrequest@example.com?subject=unsubscribe>,
    <https://example.com/unsubscribe.html/opaque123456789>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

Resulting POST request

```
POST /unsubscribe.html/opaque=123456789 HTTP/1.1
Host: example.com
Content-Type: multipart/form-data; boundary=---FormBoundaryjWmhtjORrn
Content-Length: 124

---FormBoundaryjWmhtjORrn
Content-Disposition: form-data; name="List-Unsubscribe"

One-Click
---FormBoundaryjWmhtjORrn--
```

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2369] Neufeld, G. and J. Baer, "The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields", RFC 2369, DOI 10.17487/RFC2369, July 1998, <http://www.rfc-editor.org/info/rfc2369>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <http://www.rfc-editor.org/info/rfc5322>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <http://www.rfc-editor.org/info/rfc6376>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[RFC7578] Masinter, L., "Returning Values from Forms: multipart/form-data", RFC 7578, DOI 10.17487/RFC7578, July 2015, <http://www.rfc-editor.org/info/rfc7578>.

Authors' Addresses

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886
United States of America

Phone: +1 831 480 2300
Email: standards@taugh.com
URI: http://jl.ly

Tobias Herkula
optivo GmbH
Wallstrasse 16
Berlin 10179
Germany

Phone: +49 30 768078 129
Email: t.herkula@optivo.com
URI: https://www.optivo.com