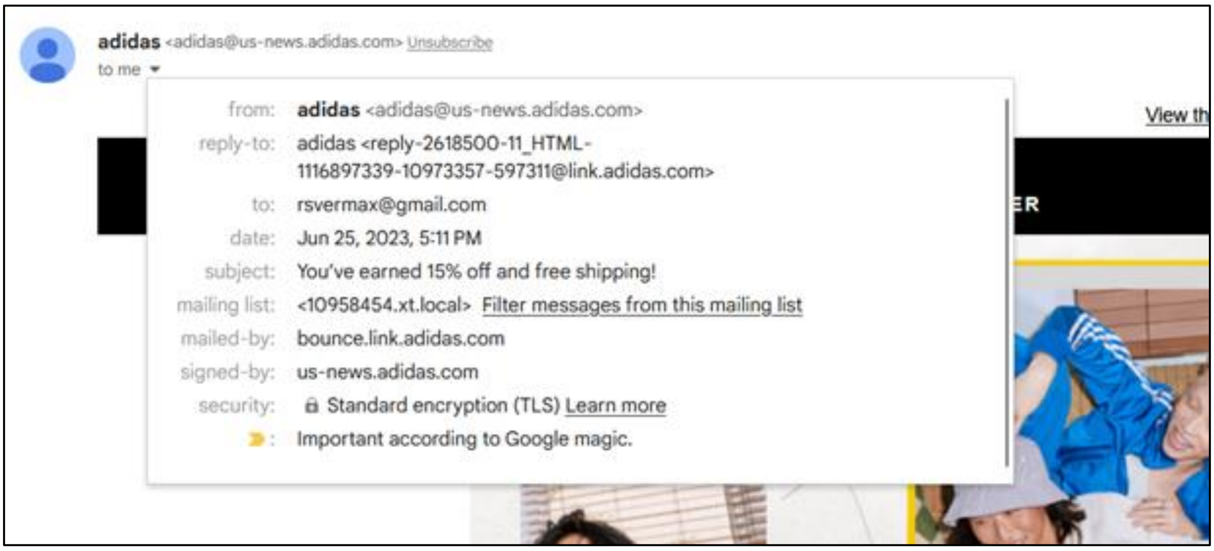
EMAIL HEADERS EXPLAINED



adidas <adidas@us-news.adidas.com> Unsubscribe

to me

from: **adidas** <adidas@us-news.adidas.com>

reply-to: adidas <reply-2618500-11_HTML-1116897339-10973357-597311@link.adidas.com>

to: rsvermax@gmail.com

date: Jun 25, 2023, 5:11 PM

subject: You've earned 15% off and free shipping!

mailing list: <10958454.xt.local> Filter messages from this mailing list

mailed-by: bounce.link.adidas.com

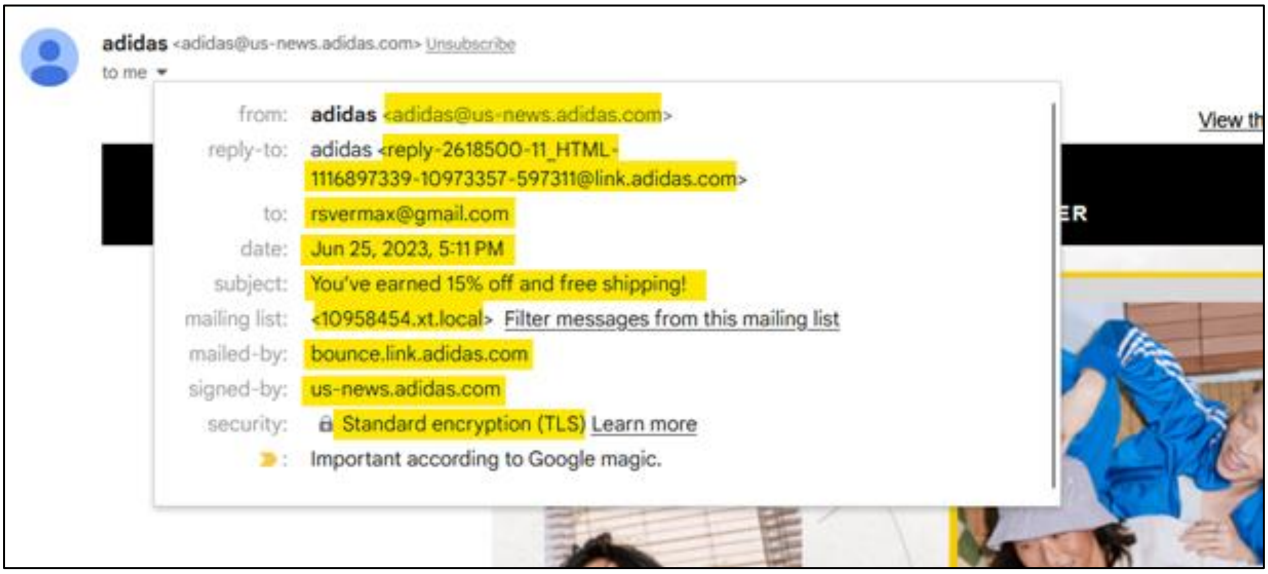
signed-by: us-news.adidas.com

security: 🔒 Standard encryption (TLS) Learn more

Important according to Google magic.

Definition:

1. From: The sender of the email is identified in this header. It contains the name and email address of the sender.
2. Reply-To: The Reply-To header indicates the intended reply address if the sender prefers that answers be sent to a different email address than the one used in the From header.
3. To: This header lists the recipients of the email. It lists the people or organizations that the email is addressed to, along with their names and email addresses.
4. Date: The time and date that the email's sender sent it are shown in this header. It aids in keeping track of the correspondence's time.
5. Subject: The email's content is briefly described or summarized in the subject header. It aids receivers in comprehending the email's goal or subject.
6. Mailing List: This header provides the name or address of the mailing list if the email was sent using a mailing list or group email address. It makes it clear that the email was sent to several recipients.
7. Mailed-By: In Gmail, the Mailed-By header contains the domain name of the email server. It displays the email client or server that the message's sender used.
8. Signed-By: The Signed-By header indicates the domain or organization that signed the email when it is digitally signed using cryptographic techniques like DKIM which is also known as DomainKeys Identified Mail. It offers a means of confirming the reliability and integrity of the communication.
9. Security: Information about the email's encryption and security mechanisms may be seen in the Security header in Gmail. It can show if a secure connection, such as TLS, was used to deliver the message or whether the email client has identified any possible security problems, like an unauthenticated sender.

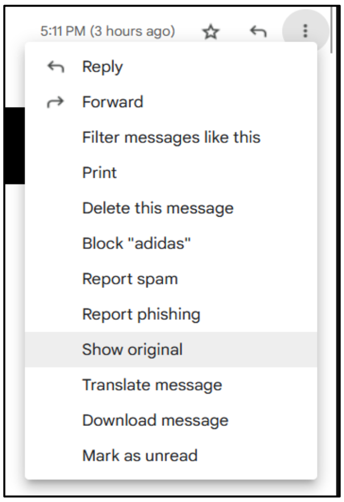


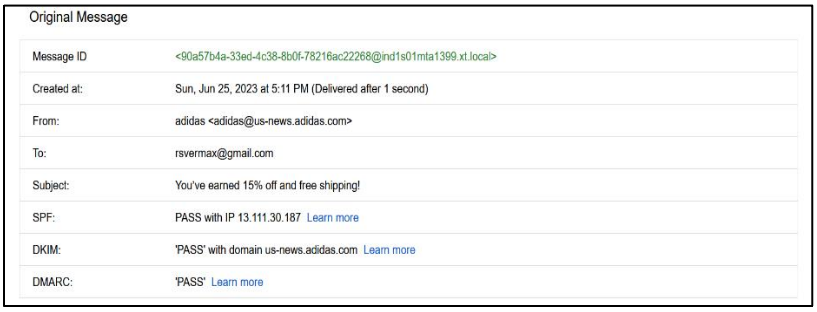
adidas <adidas@us-news.adidas.com> Unsubscribe
to me

from: adidas <adidas@us-news.adidas.com>
reply-to: adidas <reply-2618500-11_HTML-1116897339-10973357-597311@link.adidas.com>
to: rsvermax@gmail.com
date: Jun 25, 2023, 5:11 PM
subject: You've earned 15% off and free shipping!
mailing list: <10958454.xt.local> Filter messages from this mailing list
mailed-by: bounce.link.adidas.com
signed-by: us-news.adidas.com
security: Standard encryption (TLS) Learn more
: Important according to Google magic.

1. From: The Email is from ‘adidas@us-news.adidas.com’.
2. Reply-To: If we had to reply to this email the reply would be sent directly to ‘reply-2618500-11_HTML-1116897339-10973357-594311@link.adidas.com’ email address which is different from the email address we received the email from.
3. To: The email was sent to ‘rsvermax@gmail.com’.
4. Date: The time at which the email was sent was ‘Jun 25, 2023, 5:11 PM’.
5. Subject: The subject is ‘You’ve earned 15% off and free shipping!’.
6. Mailing List: Email was sent using ‘10958454.xt.local’ mailing list.
7. Mailed-By: The email client or sever Adidas used to send this email is ‘bounce.link.adidas.com’.
8. Signed-By: Adidas used ‘us-news.adidas.com’ domain to sign the email using DKIM.
9. Security: The security measure used to deliver the message is ‘standard encryption (TLS)’.

Original Message:



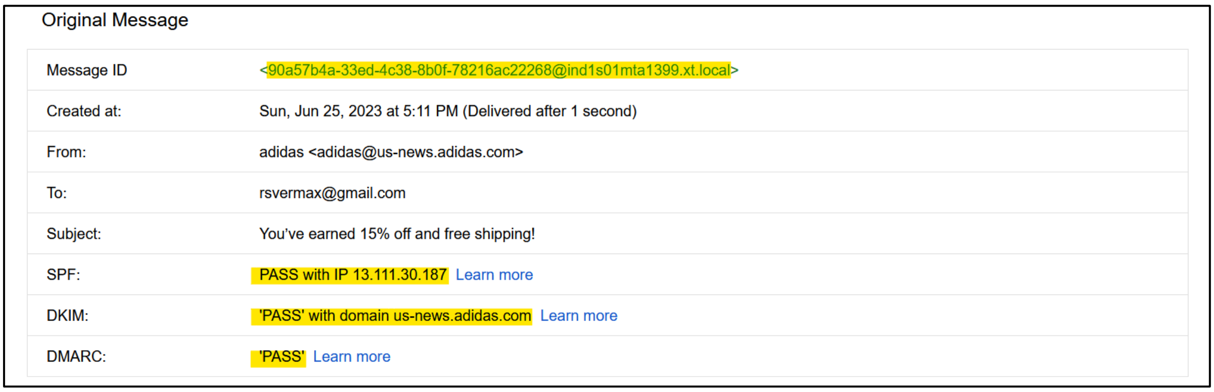


Original Message

Message ID	<90a57b4a-33ed-4c38-8b0f-78216ac22268@ind1s01mta1399.xt.local>
Created at:	Sun, Jun 25, 2023 at 5:11 PM (Delivered after 1 second)
From:	adidas <adidas@us-news.adidas.com>
To:	rsvermax@gmail.com
Subject:	You've earned 15% off and free shipping!
SPF:	PASS with IP 13.111.30.187 Learn more
DKIM:	'PASS' with domain us-news.adidas.com Learn more
DMARC:	'PASS' Learn more

We can define them as follows:

1. Message ID: Each email message is given a different identity known as the Message-ID header. It facilitates keeping track of and referring to certain emails in email threads or chats. There are about 50 letters and digits in it.
2. SPF: It is an email authentication method also known as Sender Policy Framework that verifies the sender's identity by comparing the IP address of the server delivering the email to a list of authorized IP addresses published in the DNS records of the sender's domain.
3. DKIM: Authentication mechanism that makes use of cryptographic signatures to confirm an email's authenticity and integrity is DomainKeys Identified Mail (DKIM). The digital signature sent to the email's headers or body by the sender's domain may be verified by the recipient's mail server using the public key made available in the sender's domain's DNS records.
4. DMARC: In order to provide domain owner control over how email servers handle rejected or unauthenticated emails, Domain-based Message Authentication, Reporting, and Conformance(DMARC) is a policy framework that expands upon SPF and DKIM. It allows domain owners to define the actions that recipients should take when emails fail SPF or DKIM tests.



Original Message

Message ID	<90a57b4a-33ed-4c38-8b0f-78216ac22268@ind1s01mta1399.xt.local>
Created at:	Sun, Jun 25, 2023 at 5:11 PM (Delivered after 1 second)
From:	adidas <adidas@us-news.adidas.com>
To:	rsvermax@gmail.com
Subject:	You've earned 15% off and free shipping!
SPF:	PASS with IP 13.111.30.187 Learn more
DKIM:	'PASS' with domain us-news.adidas.com Learn more
DMARC:	'PASS' Learn more

1. Message ID: The message ID is '90a57b4a-33ed-4c38-8b0f-78216ac22268@ind1s01mta1399.xt.local'.
2. SPF: Here, it says "PASS" so it's from a trusted server (Adidas official servers).
3. DKIM: Here, it says 'PASS' with domain us-news.adidas.com which means it is verified using the key available in the sender domain 'us-news.adidas.com'
4. DMARC: As it is 'PASS', it means it's from a trusted, original source and has been verified on the recipient's side as well.

SAP in SFMC:

- SAP, which is also known as Sender Authentication Package in SFMC means there is an integration between SFMC and SAP system.
- This connection enables data and information interchange between any two platforms.
- The organization's marketing and sales processes is streamlined due to this interchange, which also gives them a global picture of consumer data.
- It can consist of synchronizing client information, such as contact details and purchase history, between two systems.
- This can also be used to customize marketing efforts and target particular client segments using SAP data.
- Better data visibility, increased marketing efficacy, and a smooth user experience for both marketers and customers while utilizing both platforms concurrently are all benefits of incorporating and integrating SAP into SFMC.

Features:

1. Dedicated IP: Dedicated IP ensures that we have complete control over the IP's sending practices and reputation, by not disclosing it to other senders. Also , it helps maintain a positive sender reputation and email deliverability.
2. Private Domain: Using Private Domain we can send emails using our own custom branded domain rather than the email service provider's default domain if we already have a private domain. (e.g., Adidas uses their own braded domains, so the recipients know it's from a trusted source)
3. Image Wrapping: Here in Adidas Promotional Email, we can see all the images are directly visible to the customers so that they don't have to download any images externally which will reduce the engagement. Image Wrapping makes the images appear directly within the promotional email itself instead of downloading it from an external source.
4. Link Wrapping: This makes long appearing URLs to shorter URLs which cloud be branded links within the email itself. This eventually makes it easier for the customer and makes it easier for the organization to track the metrics of the performance.
5. Reply Mail Management: This incorporates email management for the consumer responses to that specific promotional email. We may resolve the issue utilizing a variety of techniques, and we can even send the client automated answers advising them whether the email address is a no-reply type and providing contact information.

Setting up SAP:

- Adidas uses 'adidas.com' so as to make sure the recipients can verify that it's coming from a trusted source
- Authentication is also considered, so that any kind of security breach isn't possible, this is done by using techniques like SPF, DKIM and DMARC, as we can see in the example on page 3.
- Adidas also modifies 'adidas.com' DNS entries so that it includes addition of specific DNS records to facilitate email authentication. Adidas also performs validation of DNS modifications and proper configuration of authentication protocols for adidas.com
- They can configure the Sender Profiles, From Addresses and Sending Classification.