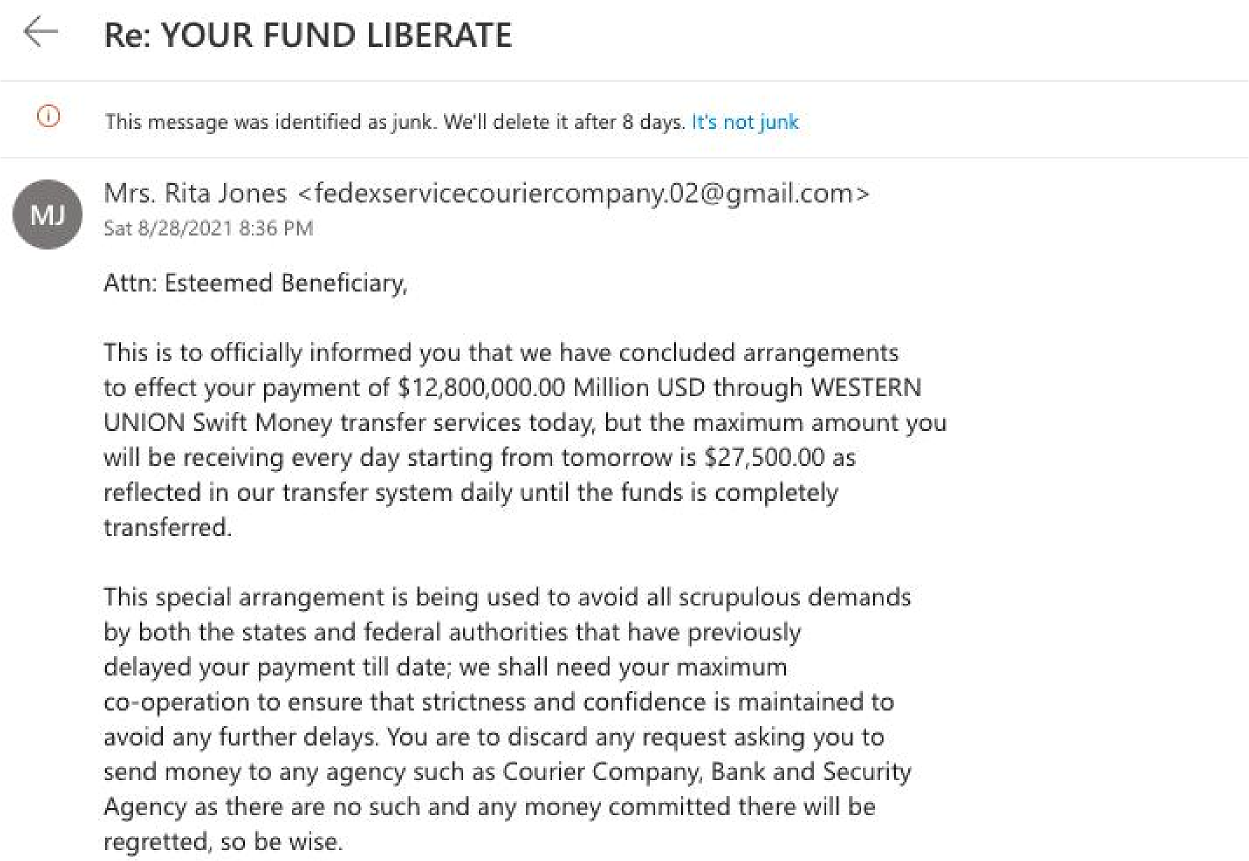
3 Ways to Check if an Email Is Real or Fake

If you've received an email that looks a bit dubious, it's always best to check its authenticity. Here are three ways to tell if an email is real.

Have you ever come across any email that looks like it's from a company, but it looked suspicious? There are plenty of ways that scammers use to spoof email addresses.

Here, we're going to cover a few ways you can identify authentic emails from fake ones.

1. Check the “From” Address



Re: YOUR FUND LIBERATE

This message was identified as junk. We'll delete it after 8 days. It's not junk

Mrs. Rita Jones <fedexservicecouriercompany.02@gmail.com>
Sat 8/28/2021 8:36 PM

Attn: Esteemed Beneficiary,

This is to officially informed you that we have concluded arrangements to effect your payment of $12,800,000.00 Million USD through WESTERN UNION Swift Money transfer services today, but the maximum amount you will be receiving every day starting from tomorrow is $27,500.00 as reflected in our transfer system daily until the funds is completely transferred.

This special arrangement is being used to avoid all scrupulous demands by both the states and federal authorities that have previously delayed your payment till date; we shall need your maximum co-operation to ensure that strictness and confidence is maintained to avoid any further delays. You are to discard any request asking you to send money to any agency such as Courier Company, Bank and Security Agency as there are no such and any money committed there will be regretted, so be wise.

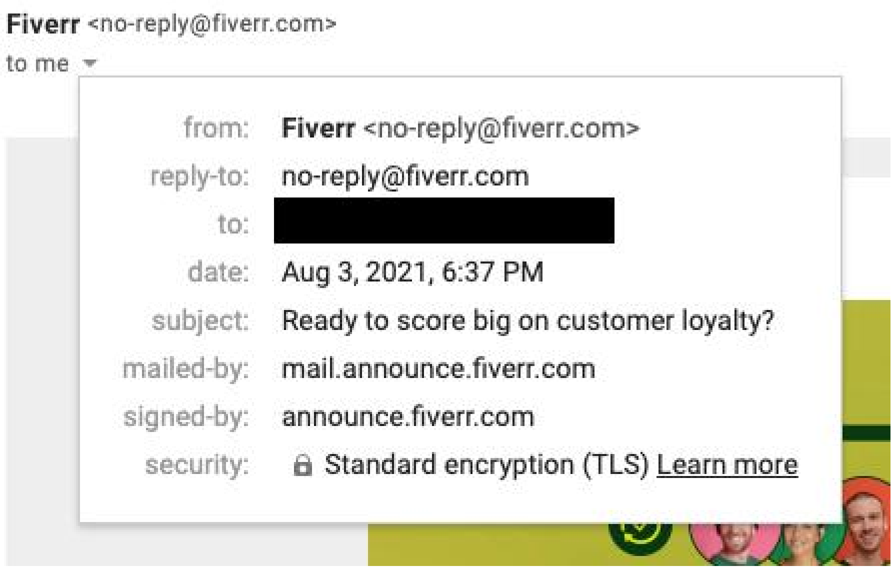
Often you'll find that fake emails that have a similar-looking “from” address to the original email addresses.

Take the example of Apple. If you receive an email from Apple, you will see that the email address is noreply@apple.com. Scammers would use similar email addresses such as noreply@appleinc.com to try and fool the recipient.

Another example is the way scammers type the name of reputed companies to scam the public. For example, they could misspell Microsoft using an 'r' and an 'n' to make it look like an 'm'.

Alternatively, scammers could use different blocks or spoofing software to show you the legit email address. In this case, it's much harder to tell if the email is real or not. Telltale signs include any spelling mistakes in the email, or suspicious looking links.

2. Check the “Reply To” Address



Fiverr <no-reply@fiverr.com>
to me

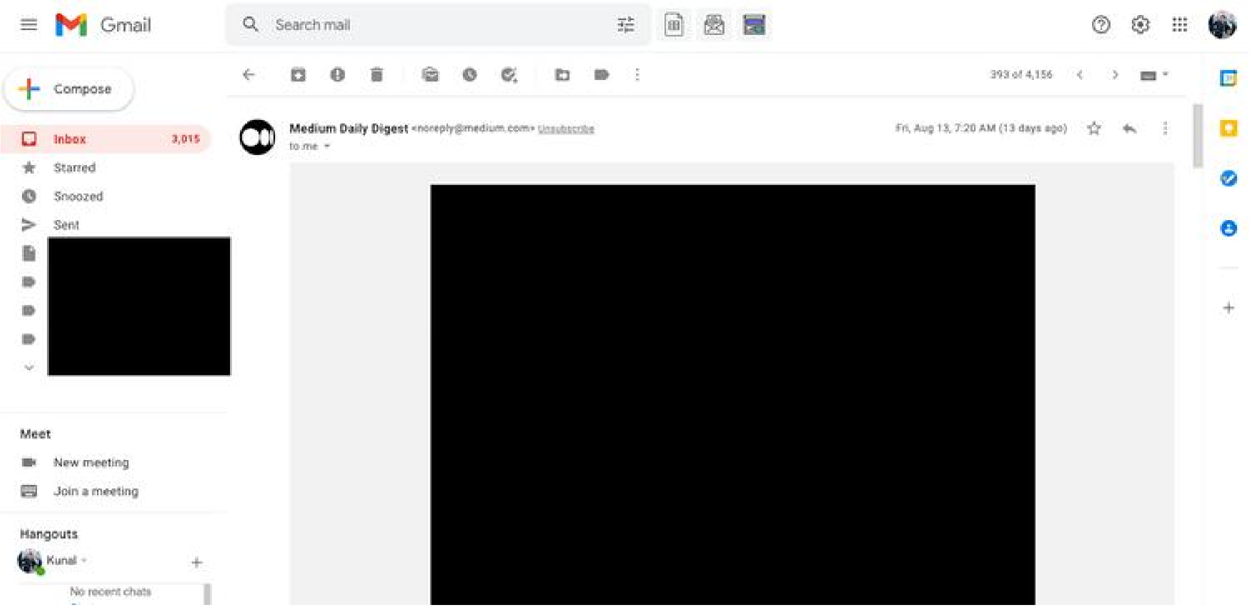
from: Fiverr <no-reply@fiverr.com>
reply-to: no-reply@fiverr.com
to: [redacted]
date: Aug 3, 2021, 6:37 PM
subject: Ready to score big on customer loyalty?
mailed-by: mail.announce.fiverr.com
signed-by: announce.fiverr.com
security: 🔒 Standard encryption (TLS) Learn more

When you receive an email from someone, you typically reply to the same email address, unless otherwise instructed. When scammers send fake emails using someone else's email addresses, they don't have access to the victims' email accounts whose name they use.

If a scam email needs a reply from you, you'll see that the “Reply To” field has a different email address than the one that actually sent you the email.

Scammers use this technique to get replies by enticing you to read and respond to the emails they send using the names of reputed brands, companies, governmental organizations, and so on.

3. Check Email Headers



Medium Daily Digest <noreply@medium.com> Unsubscribe
to me
Fri, Aug 13, 7:20 AM (13 days ago)

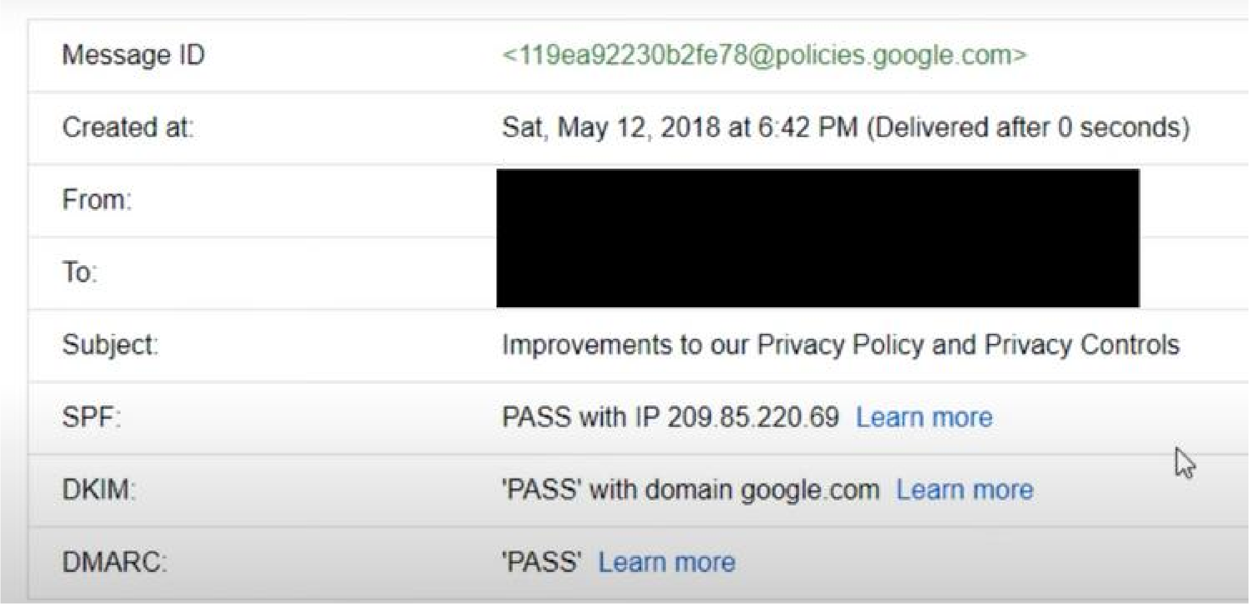
[redacted]

[redacted]

There are three major email security technologies used– SPF, DKIM, and DMARC. These technologies help the recipients of the emails check whether it is really from the recipient, or a scammer instead.

Most major websites and companies utilize these three security measures correctly, as it allows your mail client to detect and block fake emails. It's worth bearing in mind that some companies may not use these technologies or enforce them properly.

To check the security of an email, click the three dots in the top-right corner of any suspicious email and click on Show Original (or equivalent). Here, you'll be able to see each of the security checks and whether the email has passed or failed.



Message ID	<119ea92230b2fe78@policies.google.com>
Created at:	Sat, May 12, 2018 at 6:42 PM (Delivered after 0 seconds)
From:	[redacted]
To:	[redacted]
Subject:	Improvements to our Privacy Policy and Privacy Controls
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain google.com Learn more
DMARC:	'PASS' Learn more

Why Should You Check Your Emails?

You might be wondering why your email doesn't automatically check and filter out spam and fake emails with so many checks, firewalls, and layers of security out there. The answer to this question is that out of 140 million domains recently checked in a survey by SPF, 80 percent had no SPF records, which are the bare minimum for security.

Without SPF records, there's no way for your email account to accurately filter out spam messages. That's why you sometimes find important emails in your Junk folder, and the odd spam email in your Inbox.

No single test or sign can tell you that an email is authentic or suspicious for sure. You might have to do multiple tests to figure out whether an email is genuine or not.

It's Always Best to Check Suspicious Emails

You should always check the things mentioned above when you feel that you have received a suspicious email. Hacking, scamming, and online frauds are becoming more common as time passes. Scammers dupe the innocent public who know little to nothing about technology by using different techniques.

In the future, the number of spoof emails will only go upwards due to the significant shift towards digitalization. Use caution and check when in doubt.

Reference: makeuseof.com