



Email phishing

EMAIL PHISHING

----- Forwarded message -----

From: "Account Review Departmen <support@paypa1.com>"

Cc:

Bcc:

Date: Fri, 9 Jan 2026 16:30:18 +0100 (CET)

Subject: Action Required: Verify Your Account to Avoid Suspension

Dear Valued Member,

We have detected unusual activity on your account. To secure your account and prevent permanent suspension, you must verify your identity immediately. Please click the button below to complete the verification process.

Verify Now :- <http://secure-account-verify.com/>

If you ignore this request, your account will be permanently locked within 24 hours.

We regret any inconvenience this may cause you.

Sincerely,

The Account Review Team

↩ Reply

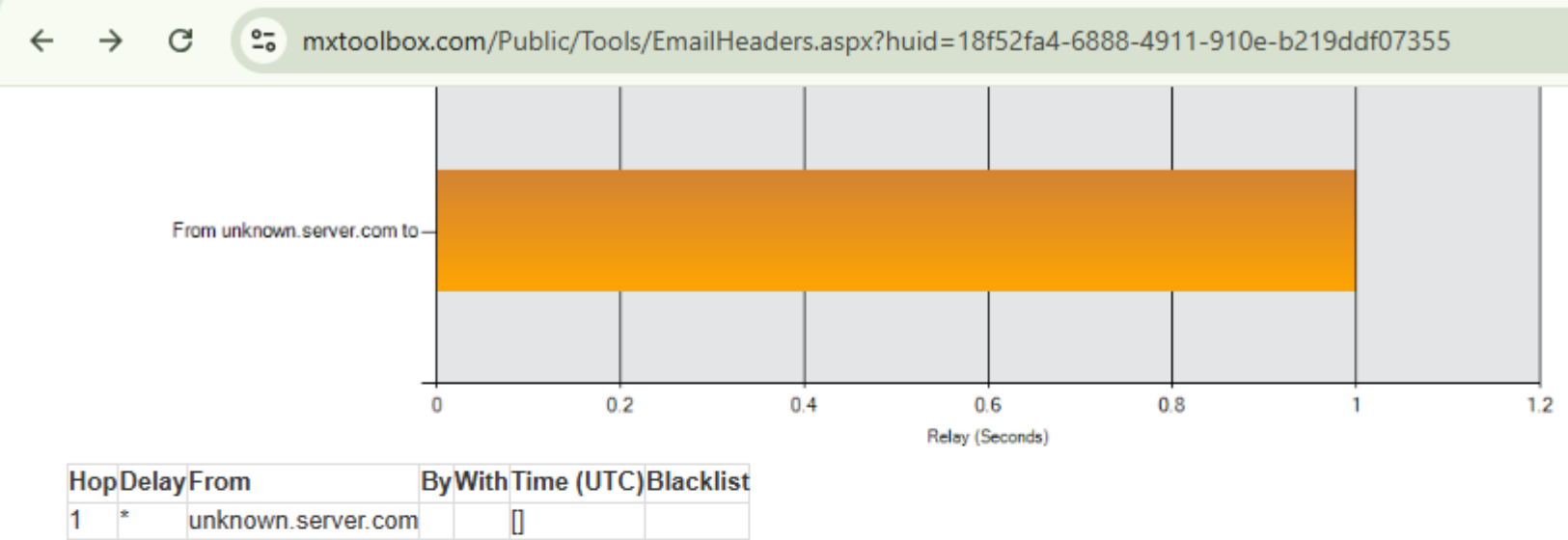
➡ Forward

😊

Indicator	Result
Fake sender domain	Yes
Urgency language	Yes
HTTP link	Yes
Generic greeting	Yes



Email Classification: PHISHING – HIGH RISK



[Gmail & Yahoo](#) are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

Headers Found

Header Name	Header Value
From	security@secure-account-verify.com
Return-Path	fake@secure-account-verify.com

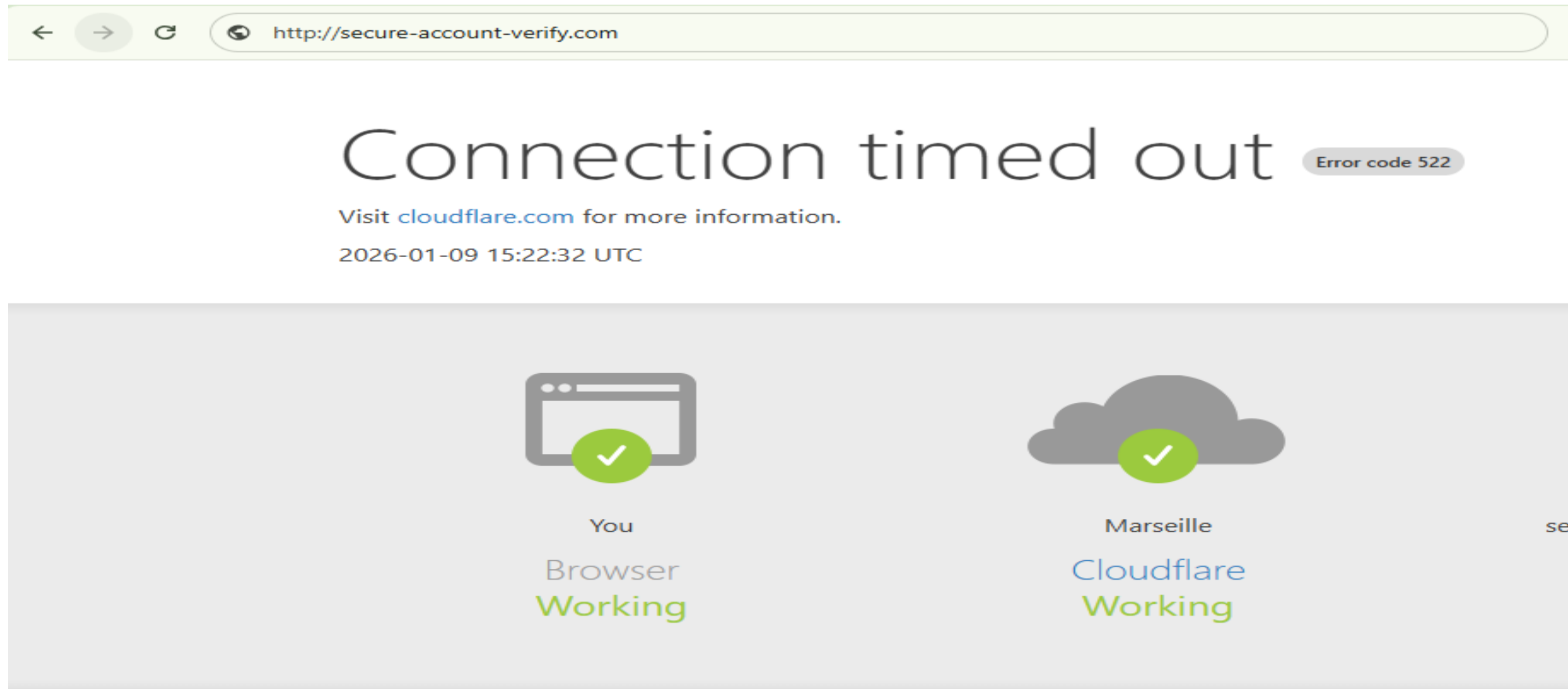
Received Header

From: security@secure-account-verify.com
Received: from unknown.server.com
Return-Path: fake@secure-account-verify.com

[Permanently forget this email header](#)



FAKE DOMAIN



What happened?

What can I do?

Prevention Guidelines Page

Do's

Check sender domain

Hover over links

Report phishing

Don'ts

Don't click unknown links

Don't share password

Don't trust urgent emails

Awareness Guidelines (Don'ts)

Don'ts

Don't click unknown links

Don't share credentials

Don't panic

Don't download attachments blindly

Example

Avoid clicking links from unverified emails

Never send passwords or OTP over email

Don't act under fear or urgency imposed by email

Only open attachments from trusted senders



Thank you