

Email Authenticity

Objective:

Provide verifiable information about the origin of email messages by validating the domain ownership of any message transfer agents who participate in transferring and possibly modifying a message.

Methodology:

- Checking the main source properly
- Any link within the mail could be suspicious
- Be cautious before clicking on any links
- Scan any suspicious attachments/links before opening

Tools:

- virustotal.com
- expandurl.net

Proof of concept (POC):

The screenshot shows an email inbox with a single message. The message is a forwarded email from Instagram security. The subject line is "Fwd: cm_fashion_online_shopping, we've made it easy to get back on Instagram". The message body is a template for password recovery, addressed to "cm_fashion_online_shopping". The message includes standard TLS encryption information and a note about Google magic. The email is dated Saturday, June 10, 2023, at 5:26 PM, and is from BibekShah00@gmail.com.

Fwd: cm_fashion_online_shopping, we've made it easy to get back on Instagram

Chandrika sah <chandrika143sah@gmail.com>
to BibekShah00@gmail.com

----- Forwarded message -----
From: Instagram <security@...>
Date: Sat, Jun 10, 2023, 5:33 AM
Subject: cm_fashion_online_shopping, we've made it easy to get back on Instagram
To: <chandrika143sah@gmail.com>

from: Chandrika sah <chandrika143sah@gmail.com>
to: "BibekShah00@gmail.com" <BibekShah00@gmail.com>
date: Jun 10, 2023, 5:26 PM
subject: Fwd: cm_fashion_online_shopping, we've made it easy to get back on Instagram
mailed-by: gmail.com
signed-by: gmail.com
security: Standard encryption (TLS) [Learn more](#)
►: Important according to Google magic.

Hi cm_fashion_online_shopping,
Sorry to hear you're having trouble logging into Instagram. We got a message that you forgot your password. If this was you, you can get right back into your account or reset your password now.

Results for https://bit.ly/3sZA2Bx

	Title: Support : NOISE
Short URL: https://bit.ly/3sZA2Bx	Redirects: 2 (show details)
Long URL: https://support.gonoise.com/support/home	

Extra Information

Meta Keywords: No Keywords
Content-Type: text/html; charset=utf-8
Canonical URL: https://support.gonoise.com/support/solutions
Google Safe Browsing: - This link appears to be safe! Advisory provided by Google.

3 security vendors flagged this URL as malicious

https://bit.ly/3sZA2Bx
bit.ly
multiple-redirects

Status 200 | Last Analysis Date 9 months ago |

Community Score 3 / 91

DETECTION **DETAILS** **LINKS** **COMMUNITY**

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis		Do you want to automate checks?	
CMC Threat Intelligence	Malicious	Comodo Valkyrie Verdict	Malware
CRDF	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira	Clean

Conclusion:

A spoofed mail with a carefully constructed message can be quite a potential threat. It can prove difficult even impossible for an everyday user to identify one as fraudulent.