

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.

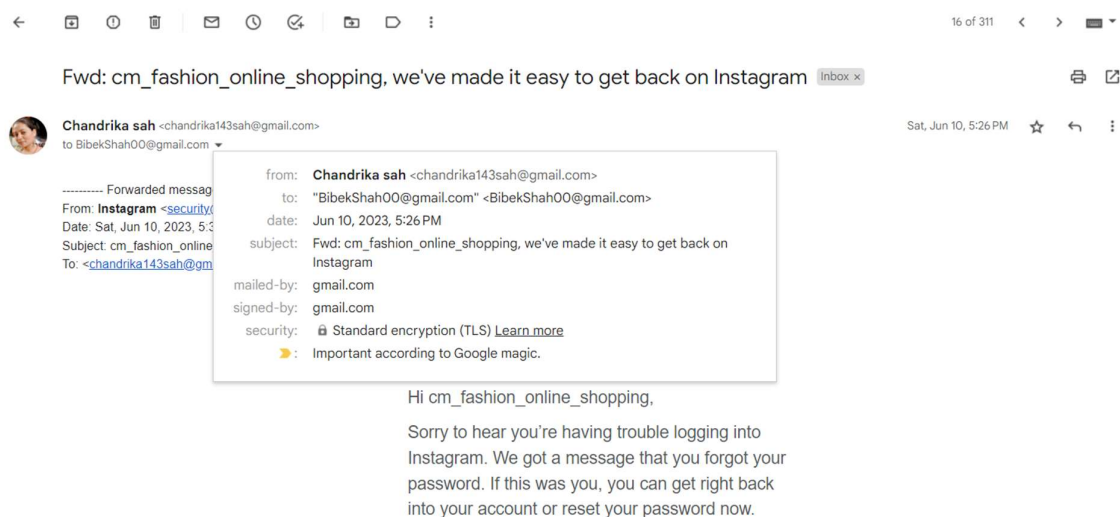
Methodology:

- 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):




expandurl.net/expand

roadmap - GitMind Subdomain Finder - One-Liner Scripts f...


ExpandURL EXPAND URL SHORTEN URL TERMS OF USE BROWSER EXTENSION CONTACT US

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.

virustotal.com/gui/url/d99a4a7da30647de43d634697cdd5c003958925bb0f3ff2172784c1a5fd852e

roadmap - GitMind Subdomain Finder - One-Liner Scripts f...

<https://bit.ly/3sZA2Bx> Sign in Sign up



3 security vendors flagged this URL as malicious

Reanalyze Search Graph API













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

Status: 200 Last Analysis Date: 9 months ago

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

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

Do you want to automate checks?

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.