

# **Phishing Email**

The Super Bowl ad that changed advertising

Today in History <newsletter@mail.britannica.com>

Why is this message in spam? You unsubscribed from this mailing list so these messages are sent to Spam. To send these messages to your inbox instead, report this message as not spam.

[Report not spam](#)

A Britannica Newsletter

Today in History

JANUARY 22, 2026

Apic—Hulton Archive/Getty Images

## The Moment Advertising Became Cinema

JANUARY 22, 1984

On this day in 1984, a new kind of television commercial quietly made history. Apple Computer's now-legendary "1984" ad became just as famous for what it didn't say as for what it *did* say.

But the commercial almost didn't see the light of day.

Airing during Super Bowl XVIII, the 60-second ad showed no products, mentioned no

[Reply](#) [Forward](#) [Print](#)

Thu, Jan 22, 4:15 PM (2 days ago) [Star](#) [Smile](#) [Share](#) [More](#)

[Reply](#) [Forward](#) [Delete](#) [Mark as unread](#) [Block "Today in History"](#) [Report phishing](#) [Filter messages like this](#) [Translate](#) [Print](#) [Download message](#) [Show original](#)

### Original Message

Message ID	<42.CF25022.5BFF1796@i-01d144fb788d85f86.mta1rest.sd.prd.sparkpost>
Created at:	Thu, Jan 22, 2026 at 4:15 PM (Delivered after 1 second)
From:	Today in History <newsletter@mail.britannica.com>
To:	moulimorampudi@gmail.com
Subject:	The Super Bowl ad that changed advertising
SPF:	PASS with IP 147.253.210.16 <a href="#">Learn more</a>
DKIM:	'PASS' with domain mail.britannica.com <a href="#">Learn more</a>
DMARC:	'PASS' <a href="#">Learn more</a>

[Download Original](#)

[Copy to clipboard](#)

```

Delivered-To: moulimorampudi@gmail.com
Received: by 2002:a05:7108:3e0b:b0:4c2:938a:b08b with SMTP id hk11csp364450gdb;
    Thu, 22 Jan 2026 02:45:18 -0800 (PST)
X-Received: by 2002:a05:690c:4990:bb:794:f67:d572 with SMTP id 00721157ae682-7940fb7fae9mr6609729b3.66.1769078710553;
    Thu, 22 Jan 2026 02:45:18 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
b=OzufJ38pfyFnw5xQ1lkdxBpvc5V868DAGmBUoBzVmQj+MCVNDXCQN550ABY+0xG
jZpXKwqXK6AVGAv7D5j46p6Bz7MfyWSRAUco3PsddvD1HLKaT0wy8rmv20HwfQz7q
5kL68sgj)U3D1VYe0rMzbhdezfhcrn9FevKskWfmngkv4W4N40YpGEdaakm3qesklu
y1rDf0t3R5sSNBd44enDpb98d2cayf7Gd7Bn+<C0194C3X8DP139EcC/mNh3gU2
TBERpJL4r8/dhEqxi38hgk1gJ0dh2zc1qgLVExAC-DsVV9n+<9681ul+puGm1Pfva
NRPo==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
b=OzufJ38pfyFnw5xQ1lkdxBpvc5V868DAGmBUoBzVmQj+MCVNDXCQN550ABY+0xG
jZpXKwqXK6AVGAv7D5j46p6Bz7MfyWSRAUco3PsddvD1HLKaT0wy8rmv20HwfQz7q
5kL68sgj)U3D1VYe0rMzbhdezfhcrn9FevKskWfmngkv4W4N40YpGEdaakm3qesklu
y1rDf0t3R5sSNBd44enDpb98d2cayf7Gd7Bn+<C0194C3X8DP139EcC/mNh3gU2
TBERpJL4r8/dhEqxi38hgk1gJ0dh2zc1qgLVExAC-DsVV9n+<9681ul+puGm1Pfva
wUlviw0aEFCY1c99165+dee>xHWm289M01ATwNt74BnA83400Pm/01zw1lW0Ddc

```

Google search results for "eml analyzer":

- EML Analyzer**  
https://eml-analyzer.herokuapp.com/
- Sublime EML Analyzer**  
https://analyzer.sublime-security.com/

No information is available for this page.

**EML Analyzer** Home Cache API GitHub Cache VirusRep VirusTotal Unbounce

• EML (.eml) and MSG (.msg) formats are supported.  
 • The MSG file will be converted to the EML file before analyzing. The conversion might be lossy.  
 • This app doesn't store EML/MSG file you upload.

Drop the EML/MSG file here or click to upload

Covers and Build-a-thon.eml

Analyze

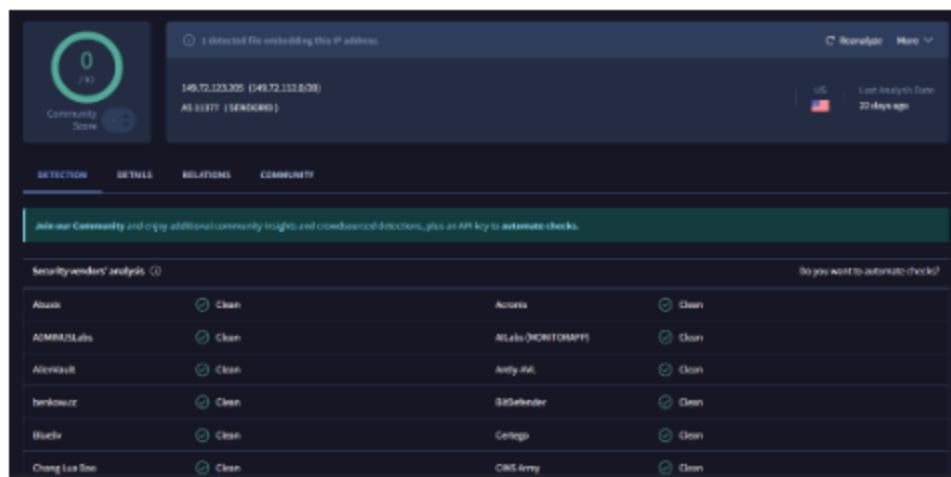
## Headers

### Hops

Hop	From	By	With	Date (UTC)	Delay
1			http://d1theclub/sublime-analyzer/29-aug-2025-2105001479+0000 (utc)	Invalid Date	N/A
2			envelope-id: 7881649b-19w-1-n@21624-85-2025-08-29-21050040004915+0000 (utc) msg+7446/41510 19/189	Invalid Date	N/A
3	o1 mail.beethilv.com, 149.72.129.05	mx.google.com	envelope-id: ca19c2360f4ec-8871e34a089b42548390912025-08-29-14-06-13	2025-08-29T21:06:13Z	N/A
4	2002:aef5b88d01b073351b5f01e	smtp.id.e1ksp631265pi		2025-08-29T21:06:14Z	N/A



The image shows the VirusTotal search interface. At the top, there is a large logo consisting of a stylized 'Σ' symbol followed by the word 'VIRUSTOTAL'. Below the logo, a subtitle reads: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." A navigation bar with tabs for "FILE", "URL", and "SEARCH" is visible. The "SEARCH" tab is currently selected. In the center, there is a search bar containing the IP address "149.72.123.205". Below the search bar is a search button labeled "Search".



The image shows the detailed analysis results for the IP address 149.72.123.205. The results are presented in a card format. At the top left is a circular "Community Score" icon showing a value of 0/97. To its right, it says "3 detected file embedding this IP address". Below this, the IP address is listed as "149.72.123.205 (149.72.123.205)" and "AS 51377 (SENDGRID)". On the right side, there is a "US" flag and "Last Analysis Date: 22 days ago". Below the main card, there are tabs for "SILENTION", "DETAILS", "RELATIONS", and "COMMUNITY". A green banner below these tabs encourages users to "Join our Community and copy additional community insights, and crowdsourced detections, plus an API key to automate checks." At the bottom, there is a table titled "Security vendors' analysis (0)" with columns for vendor name and status. The table lists several vendors: Abuse, Clean; ATIRRIUSLabs, Clean; AlienVault, Clean; Berkasoz, Clean; Bucliv, Clean; and Chong Lai Ben, Clean. To the right of the table is a section asking "Do you want to automate checks?" with a "Yes" button.