

Task :-Analyze a Phishing Email sample

Steps :-

Step 1. Obtain a sample phishing mail (u may get in online)

-This is the fake phishing email that I have

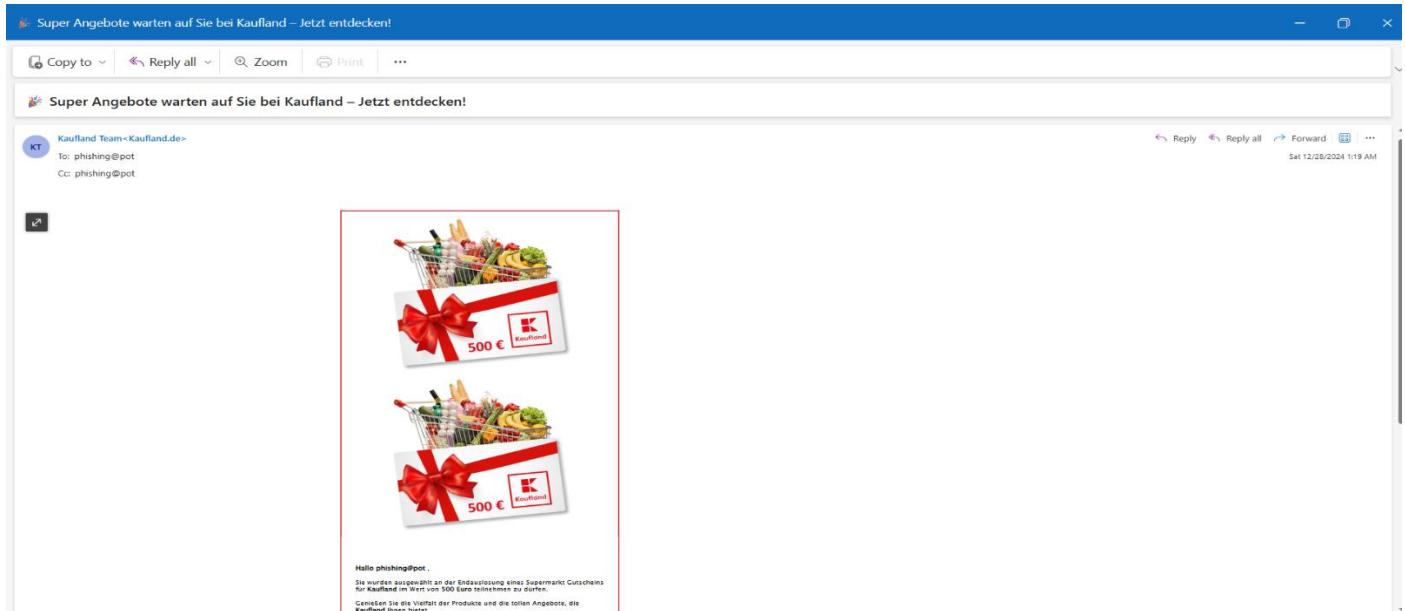


Fig 1-sample phishing mail

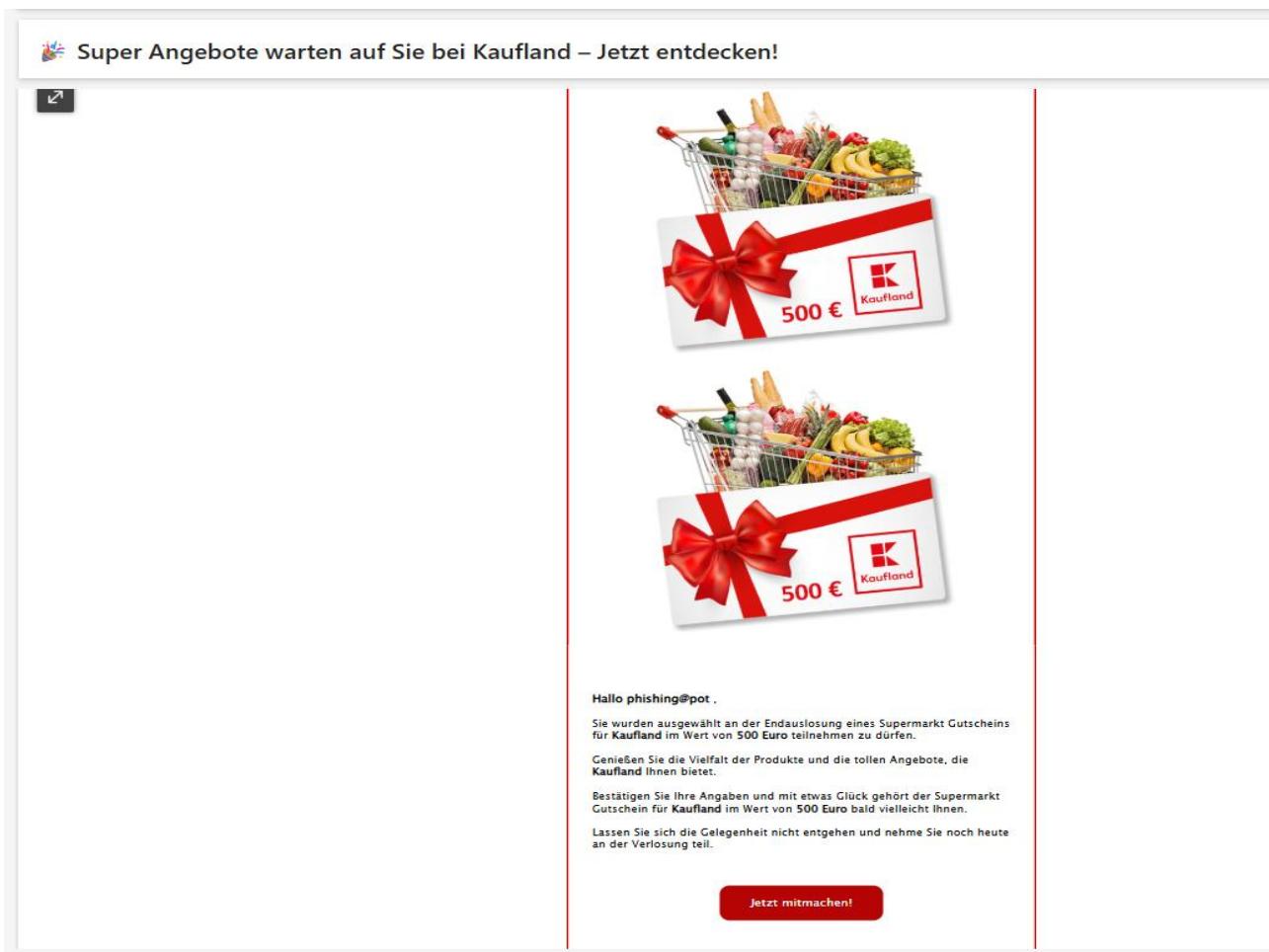


Fig 1.1

Step 2. Examine sender's email address for spoofing

Steps	What to Check	Why It Matters
1	Visible Name vs Actual Address	Attackers use familiar names with fake domains (e.g. Kaufland Team <fake@scam.com>)
2	Check Domain Authenticity	Is the domain (@something.com) a legitimate domain of the claimed sender?
3	Look for Homoglyphs	E.g. replacing I with l or using rn instead of m
4	Inspect SPF/DKIM/DMARC in the headers	These email security records confirm if the sender is authorized
5	Review IP address of sender	Cross-check whether it's from a trusted company server
6	Search domain on WHOIS or VirusTotal	To check reputation of the sending domain

-these are steps should be done to examine senders email address for spoofing

-use EML Analyzer

- Open it
- Just paste or drop the email that u want to check

The screenshot shows the Sublime Security EML Analyzer interface. On the left, there's a sidebar with information about the tool, including its purpose (automatically analyze EML to quickly investigate suspicious emails), how it works (parses raw email messages into a structured schema), and prevent attacks (blocks attacks and automates phishing investigations). The main area is titled "EML Analyzer" and contains an "Analysis Summary" section. The "Attack Score" is shown as "Malicious". Below this, there are sections for "Attack Score Verdict" (Malicious), "Attack Score Signals" (Potential Spoof: The sender failed SPF authentication), "Authoritative Display Name" (The sender's display name resembles that of an automated system or authoritative figure, a common tactic used in credential phishing attacks or other...), and "Suspicious Subject" (The subject contains emojis that are commonly used in spam messages). At the bottom, there's a "Message Details" section with "Message Insights (13)" and a table of findings, including SPF: Fail, Mismatched Sender (From) and Return-Path: service@stayfriends.de, Domains in body: blog.afridox.com, Low reputation links (2): http://blog.afridox.com/MU13d3pOVG1zMmN..., Tracking pixel in HTML body, Domains in... (7): zpaytz.xyz, db5pepf00014b8c.mail.protection.outlook.com, and Domains in... (7): db5pepf00014b8c.mail.protection.outlook.com. The file name listed is "sample-4598.eml".

Fig 2-This EML Analyzer(when I drop my email file ,Then this was result)

-you can see the Analysis summary of it. (it is malicious file)

The screenshot shows the Sublime Security EML Analyzer interface. On the left, there's a sidebar with the title "EML Analyzer" and a section titled "How does it work?" which explains the process of parsing raw email messages into a structured schema (Message Data Model) and analyzing them using detection rules (Message Query Language). Below this, there's a note about the full Sublime platform including organizational context, history, and behavioral baselines.

The main area is titled "Message Details" and contains a table titled "Message Insights (13)". The insights listed include:

- SPF: Fail
- Mismatched Sender (From) and Return-Path: service@stayfriends.de
- Domains in body: blog.afrixox.com
- Links in body (2): <http://blog.afrixox.com/MU13d3pOVG1zMmNqVnd...>
- Microsoft CrossTenant-Network-Message-Id: 97e7e390-0373-4a56-
- Return-Path: service@stayfriends.de
- UTC offset of sender: 0
- Low reputation links (2): <http://blog.afrixox.com/MU13d3pOVG1zMmN...>
- Tracking pixel in HTML body
- Domains in... (7): zpaytz.xyz, db5pepf00014b8c.mail.protection.outlook.com
- Message-ID: <hBvCQY0.0.0.hBvCQY0.9.hBvCQY0@stayfriends.de>
- Microsoft SCL: 5
- Sender Prevalence: new

Fig 2.1-Message Details

Check	Result	Verdict
Display Name	"Kaufland Team"	Looks legitimate – but only at first glance
Email Address	service@stayfriends.de	NOT Kaufland's domain
Domain Mismatch	stayfriends.de is unrelated to Kaufland	Spoofing attempt
SPF Result	Fail	Sender IP not authorized
DKIM/DMARC	Both missing	Suspicious
Sender IP	45.143.92.114	Not from Kaufland servers
WHOIS / Reputation	IP & domain have poor reputation	Bad actor likely involved

-you can check the Display name ,email address ,domain mismatch, Spf Result ,IP address etc

-you can check out Message ID (fig 2.1)

-you can get URL links (fig 2.1)

-Analyze the sender and return path (fig 2.1)



Fig 2.2-Link preview(you can see the original and effective URL)

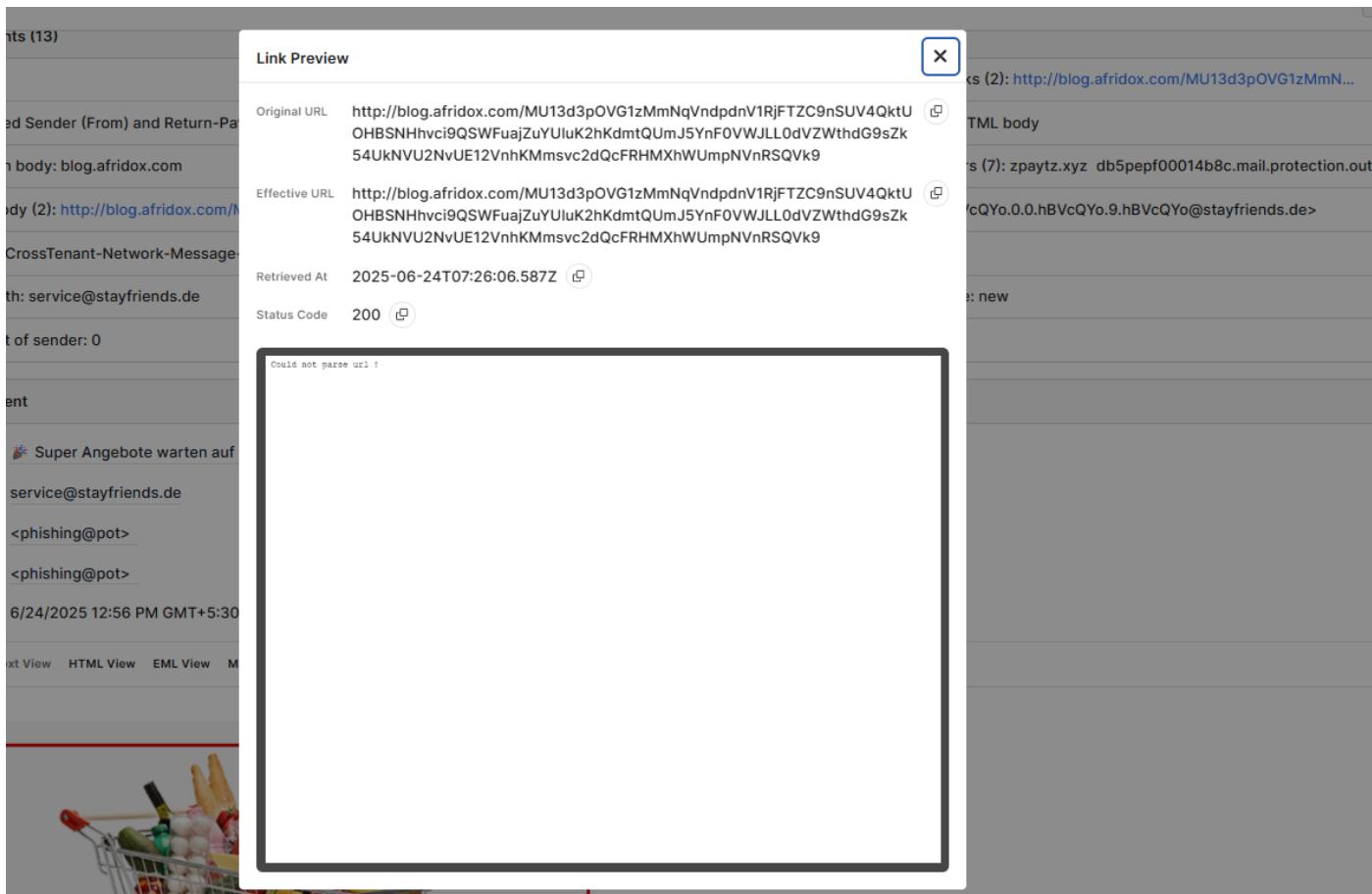


Fig 2.3-Link preview(you can see the original and effective URL)

Step 3. Email Header Discrepancy Analysis Report

1. From Address vs Return-Path

- From: Kaufland Team <service@stayfriends.de>
- Return-Path: service@stayfriends.de

Discrepancy Identified: While the display name impersonates the brand "Kaufland", the actual sending domain stayfriends.de is unrelated and unaffiliated with Kaufland. This is a clear case of brand impersonation.

Conclusion:

Spoofing attempt detected – Misleading use of branding to deceive the recipient.

2. SPF (Sender Policy Framework) Validation

- Authentication-Results:
- Spf = fail (sender IP is 45.143.92.114)
- Received-SPF: Fail – domain stayfriends.de does not designate 45.143.92.114 as a permitted sender

Discrepancy Identified: The IP address used to send this email is not listed in the SPF record of the sender's domain, causing the SPF check to fail.

Conclusion:

SPF failure – The sender is not authorized to send on behalf of stayfriends.de, indicating possible email forgery.

3. DKIM and DMARC Authentication Status

- DKIM: Not present
- DMARC: Not present

Discrepancy Identified: The email lacks both DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting & Conformance) authentication.

Conclusion:

Authentication missing – Absence of these security mechanisms increases the likelihood of spoofing and reduces traceability.

4. Received Headers (Message Routing Path)

- Mail Path Includes:zpaytz.xyz (45.143.92.114)

- Microsoft Exchange servers (e.g., DUZPR01CA0233.eurprd01.prod.exchangelabs.com)

Discrepancy Identified: The message originates from zpaytz.xyz, a suspicious and unrelated third-party domain, before passing through Microsoft infrastructure. This domain is not associated with the claimed sender or recipient environment.

Conclusion:

Untrusted mail path – Use of a suspicious domain (zpaytz.xyz) in the initial hop is indicative of potential malicious infrastructure.

5. X-Sender-IP & Spam Confidence Level (SCL)

- X-Sender-IP: 45.143.92.114
- Spam Confidence Level (SCL): 5

Discrepancy Identified: The sender IP belongs to a known spam-associated block range. Additionally, the SCL score of 5 indicates that Microsoft's spam filter has flagged the message as suspicious.

Conclusion:

Known spam source – Message likely originated from a high-risk sender.

:this is another step to check the user header,open any free user header analyzer ,copy the header and see the result

```
sql
Received: from BY5PR02MB6849.namprd02.prod.outlook.com (::1) by
IA1PR02MB9088.namprd02.prod.outlook.com with HTTPS; Fri, 27 Dec 2024 19:50:47 +0000
Received: from DUZPR01CA0233.eurprd01.prod.exchangelabs.com (2603:10a6:10:4b4::17)
by BY5PR02MB6849.namprd02.prod.outlook.com (2603:10a6:a03:20c::11) with Microsoft
SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
id 15.20.8293.16; Fri, 27 Dec 2024 19:50:45 +0000
Received: from DBSPEPF00014B8C.eurprd02.prod.outlook.com
(2603:10a6:10:4b4:cafe::a0) by DUZPR01CA0233.outlook.office365.com
(2603:10a6:10:4b4::17) with Microsoft SMTP Server (version=TLS1_3,
cipher=TLS_AES_256_GCM_SHA384) id 15.20.8293.16 via Frontend Transport;
Fri, 27 Dec 2024 19:50:43 +0000
Authentication-Results: spf=fail (sender IP is 45.143.92.114)
smtp.mailfrom=stayfriends.de; dkim=none (message not signed)
header.d=none; dmarc=none action=none header.from=stayfriends.de;
Received-SPF: Fail (protection.outlook.com: domain of stayfriends.de does not
designate 45.143.92.114 as permitted sender) receiver=protection.outlook.com;
client-ip=45.143.92.114; helo=zpaytz.xyz;
Received: from zpaytz.xyz (45.143.92.114) by
DBSPEPF00014B8C.mail.protection.outlook.com (10.167.8.200) with Microsoft
SMTP Server id 15.20.8293.12 via Frontend Transport; Fri, 27 Dec 2024 19:50:43 +0000
X-Sender-IP: 45.143.92.114
Return-Path: service@stayfriends.de
From: Kaufland Team <Kaufland.de>, Kaufland Team <service@stayfriends.de>
To: phishing@pot
Subject: 🎉 Super Angebote warten auf Sie bei Kaufland - Jetzt entdecken!
Date: Fri, 27 Dec 2024 19:49:58 +0000
Message-ID: <hBVcQY0.0.0.hBVcQY0.9.hBVcQY0@stayfriends.de>
MIME-Version: 1.0

```

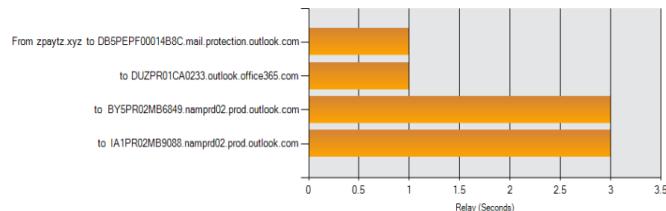
Fig 3-email header

Delivery Information

- ✖ DMARC Compliant
- ✓ SPF Alignment
- ✖ SPF Authenticated
- ✖ DKIM Alignment
- ✖ DKIM Authenticated

Relay Information

Received	4 seconds
Delay:	



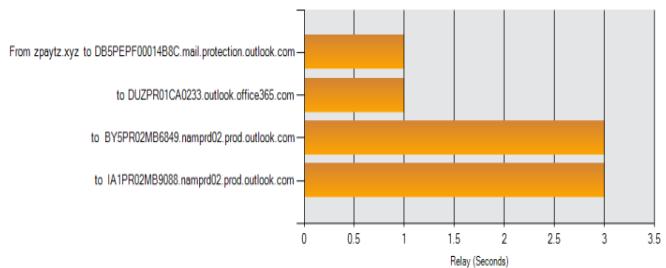
Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	zpaytz.xyz 45.143.92.114	DB5PEPF00014B8C.mail.protection.outlook.com 10.16 7.8.200	Microsoft SMTP Server	12/27/2024 7:50:4 3 PM	✖

Your IP is: 10.140.20.7 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2



Fig 3.1-Result of header analyzer

Delay:	
--------	--



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	zpaytz.xyz 45.143.92.114	DB5PEPF00014B8C.mail.protection.outlook.com 10.16 7.8.200	Microsoft SMTP Server	12/27/2024 7:50:4 3 PM	✖
2	0 seconds	DB5PEPF00014B8C.eurprd02.prod.outlook.com 2603:10a 6:10:4b4:cafe::a0	DUZPR01CA0233.outlook.office365.com 2603:10a:6:10: 4b4::17	Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384)	12/27/2024 7:50:4 3 PM	✓
3	2 seconds	DUZPR01CA0233.eurprd01.prod.exchangelabs.com 2603:1 0a6:10:4b4::17	BY5PR02MB6849.namprd02.prod.outlook.com 2603:10: b6:a03:20c::11	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	12/27/2024 7:50:4 5 PM	✓
4	2 seconds	BY5PR02MB6849.namprd02.prod.outlook.com ::1	IA1PR02MB9088.namprd02.prod.outlook.com	HTTPS	12/27/2024 7:50:4 7 PM	✖

Fig 3.2-Result of header analyzer

SPF and DKIM Information

dmarc:stayfriends.de [Show](#) [Solve Email Delivery Problems](#)

v=DMARC1; p=reject; rua=mailto:report@stayfriends.de; ruf=mailto:report@stayfriends.de; sp=reject; ri=86400

spf:stayfriends.de:45.143.92.114 [Show](#)

v=spf1 ip4:193.105.46.0/25 ip4:91.236.106.0/23 include:spf.protection.outlook.com -all

Dkim Signature Error:
No DKIM-Signature header found - [more info](#)

Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - [more info](#)

Headers Found

Fig 3.3-Result of header analyzer

Step 4.Identify the malicious Links and attachments

1. Primary Call-to-Action (CTA) Link

<http://blog.afridox.com/MU13d3pOVG1zMmNqVndpdnV1RjFTZC9nSUV4QktUOHSNHHvci9QSWFuajZuYUluK2hKdmtQUmJ5YnF0VWJLL0dVZWthdG9sZk54UkNVU2NvUE12VnhKMmsvc2dQcFRHMXhWUmpNVnRSQVk9>

- **Displayed Purpose:** "Jetzt mitmachen!" (Join Now!)
- **Actual Domain:** blog.afridox.com
- **Analysis:** This domain is **not** affiliated with kaufland.de or any legitimate company.
- **Risk:** Likely hosts a **fake form, malware, or credential-harvesting page**.

2. Unsubscribe Link

<http://blog.afridox.com/Y016MDBKTE1kdTNobkdTZ05k...>

- **Displayed Purpose:** "click here to remove yourself from our emails list"
- **Actual Domain:** Still blog.afridox.com
- **Risk:** Fake unsubscribe links are commonly used for **tracking users** or delivering malware.

3. Tracking Pixel (Hidden 1px image)

```

```

- **Purpose:** A 1-pixel image is a **common tracking mechanism** in phishing campaigns.
- **Domain:** Again, blog.afridox.com
- **Risk:** Tracks if the email was opened, which validates your address for further spam or attacks.

Attachments:-

No file attachments (.pdf, .doc, .exe, .zip, etc.) were found in this email

Item	Found?	Suspicious?	Risk Level
Malicious Links	Yes (3+)	Yes (redirect to unrelated domain)	High
Attachments	No	-	Low

Step 5.Urgent or Threatening Language in the Email Body

1. "Sie wurden ausgewählt an der Endauslosung eines Supermarkt Gutscheins für Kaufland im Wert von 500 Euro teilnehmen zu dürfen."
 - *Translation:* "You have been selected to participate in the final draw for a Kaufland supermarket voucher worth 500 euros."
 - Urgency tactic – implies exclusivity and a limited-time opportunity.
2. "Lassen Sie sich die Gelegenheit nicht entgehen und nehme Sie noch heute an der Verlosung teil." - - - *Translation:* "Don't miss this opportunity and take part in the draw today."
 - Clear pressure language – urging immediate action.
3. "Jetzt mitmachen!" (on a button)
 - *Translation:* "Join now!"
 - Classic call-to-action, pushing the reader to click immediately.

Step 6-verify the spelling or grammar errors

Spelling & Grammar Errors Found:

1. "nehme Sie noch heute an der Verlosung teil"

- **Error:** "nehme Sie"
- **Correct form:** "nehmen Sie"
- **Issue:** Incorrect verb conjugation (mixes informal/command tone)

2. "teilnehmen zu dürfen"

- **Error:** Awkward/incorrect phrase in context
- **Better:** "...an der Verlosung teilnehmen zu dürfen" or restructured entirely.
- **Issue:** Sounds machine-translated or poorly written

3. "Supermarkt Gutschein" (twice)

- **Error:** Should be "**Supermarktgutschein**" (compound noun in German)
- **Issue:** German grammar requires compound word for clarity

4. "Lassen Sie sich die Gelegenheit nicht entgehen und nehme Sie..."

- **Error:** Two issues:
 - "nehme Sie" → should be "nehmen Sie"
 - Verb order and flow are awkward.
- **Better phrased:**
"Lassen Sie sich die Gelegenheit nicht entgehen und nehmen Sie noch heute teil."

5. "click here to remove yourself..."

- **Error:** English phrase in a mostly German email
- **Issue:** Inconsistent language — suspicious for phishing

📌 Key Fields in the Email Header:

Header Field	Details
From	Kaufland Team <service@stayfriends.de>
To	phishing@pot
Subject	🎉 Super Angebote warten auf Sie bei Kaufland – Jetzt entdecken!
Date	Fri, 27 Dec 2024 19:49:58 +0000
Return-Path	service@stayfriends.de
Sender IP	45.143.92.114 (via zpaytz.xyz)
Authentication-Results	SPF=fail , DKIM=none , DMARC=none
Received-SPF	Fail — domain stayfriends.de does not authorize 45.143.92.114
Message-ID	<hBVcQYo.0.0.hBVcQYo.9.hBVcQYo@stayfriends.de>
X-MS-Exchange-SCL	5 (indicates potential spam)
List-Unsubscribe	<hBVcQYo...@stayfriends.de>
X-Microsoft-Antispam Info	Marked as suspicious; detailed analysis hash encoded

Fig 4-Key fields in email header

Step 7-summarize phishing traits found in the email

Category	Details	Red Flag
Sender Spoofing	Email is pretending to be from Kaufland , but sent from service@stayfriends.de.	Critical
Unrelated Domain	The sender's domain stayfriends.de has nothing to do with Kaufland.	Critical
Failed Authentication	- SPF: FAIL (IP not authorized) - DKIM: None - DMARC: None	Major Red Flag
Suspicious Links	Links point to domains like: http://blog.afridox.com/... — not a Kaufland domain	Critical
Unusual Sender IP	IP address: 45.143.92.114 — known to be used in spam/malware (based on public threat intelligence)	warning
Urgent Language	Offers a €500 Kaufland gift card , says: “ <i>Jetzt mitmachen!</i> ” (<i>Join now!</i>) to create urgency	warning
Email Structure	Marketing-style HTML with CTA buttons and embedded tracking pixels	warning
Impersonation	Claims to be Kaufland , but neither the sender nor the domain match	Critical
List-Unsubscribe	Contains a fake/unusual unsubscribe header that doesn't comply with standard mailing services	warning
Spam Score (SCL)	X-MS-Exchange-Organization-SCL: 5 – flagged as potential spam/phishing by Microsoft	High Risk