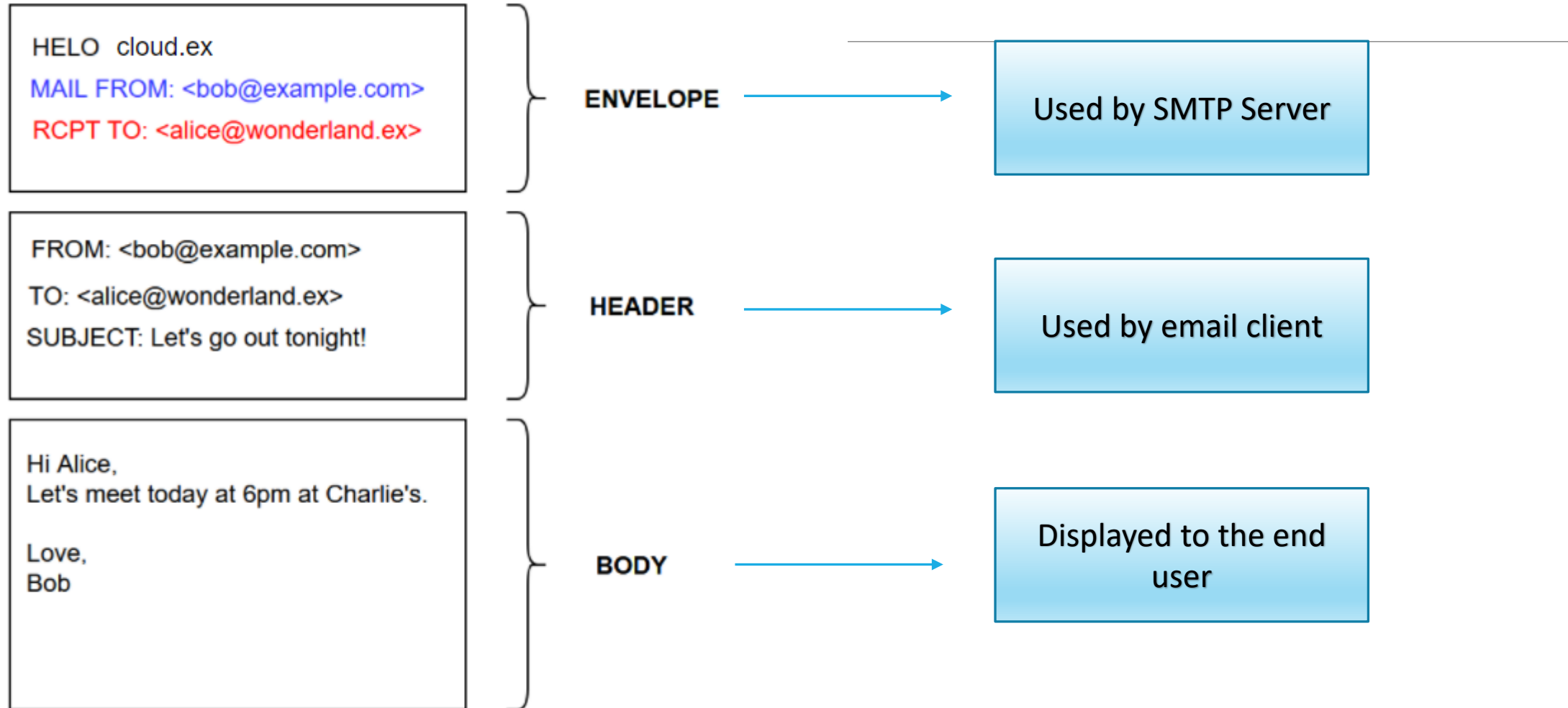




# Phishing email analysis

# Email Structure



# Email Authentication Protocols

# Email Authentication Protocols

---

## **SPF**

- TXT record on the DNS Server
- prevent spammers from sending messages on behalf of your domain

## **DKIM**

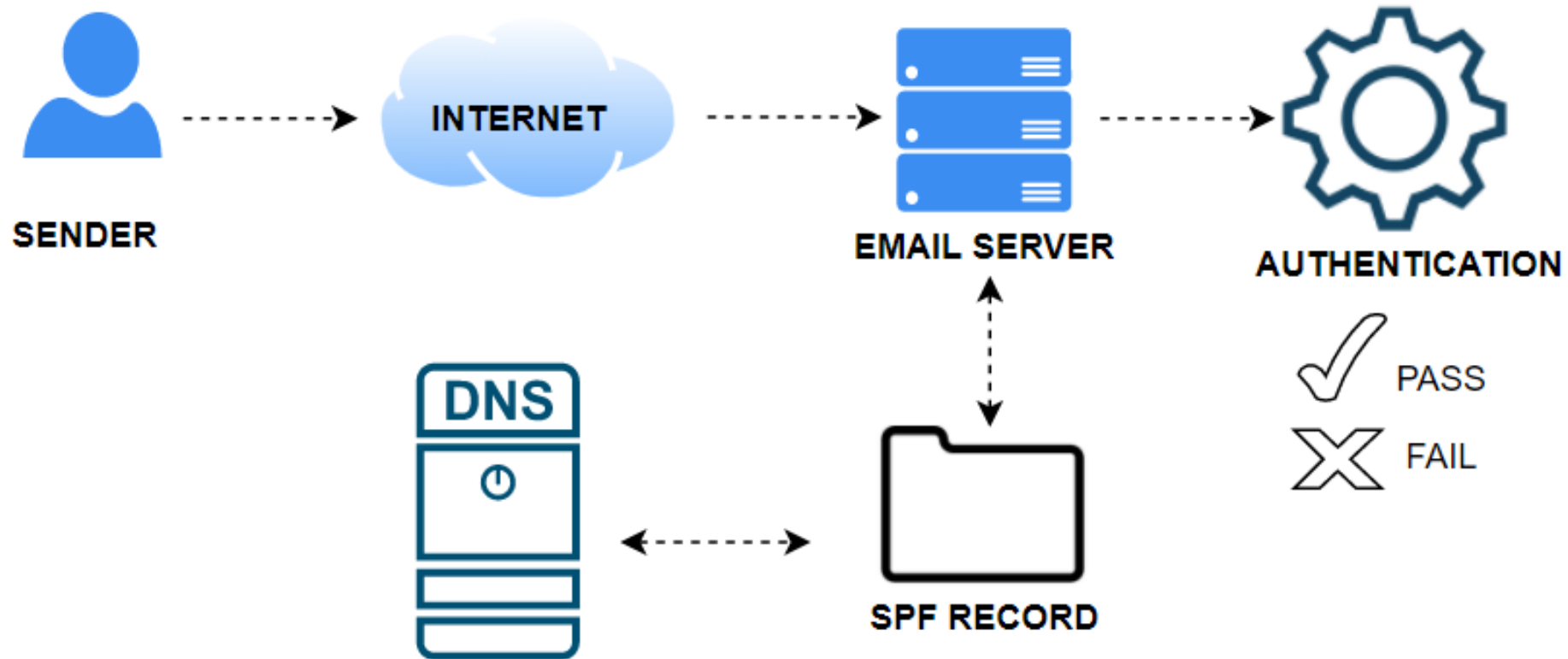
- TXT record that contains a public key used by receiving mail servers

## **DMARC**

- Is a digital signature that contains the headers and/or a body of an email

# Email Authentication protocols

## SPF



# Email Authentication protocols

## SPF - Syntax

---

**Arguments** describe the set of hosts which are designated outbound mailers for the domain

- + Pass
- - Fail (email will be rejected)
- ~ Soft fail (email will be marked)
- ? Neutral (default)
- ipv4

**Example:** v=spf1 ipv4:64.233.160.1/16 +all (Allow any IP address in range 64.233.160.1/16)

**Example:** v=spf1 -all (The domain sends no email at all)

# Email Authentication protocols

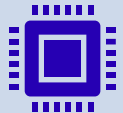
## SPF - Disadvantages



Forwarded emails fail authentication - When someone else forwards an email sent from your domain, their IP address won't be listed on your SPF record and the email will be flagged as SPF failed



SPF Records are difficult to maintain

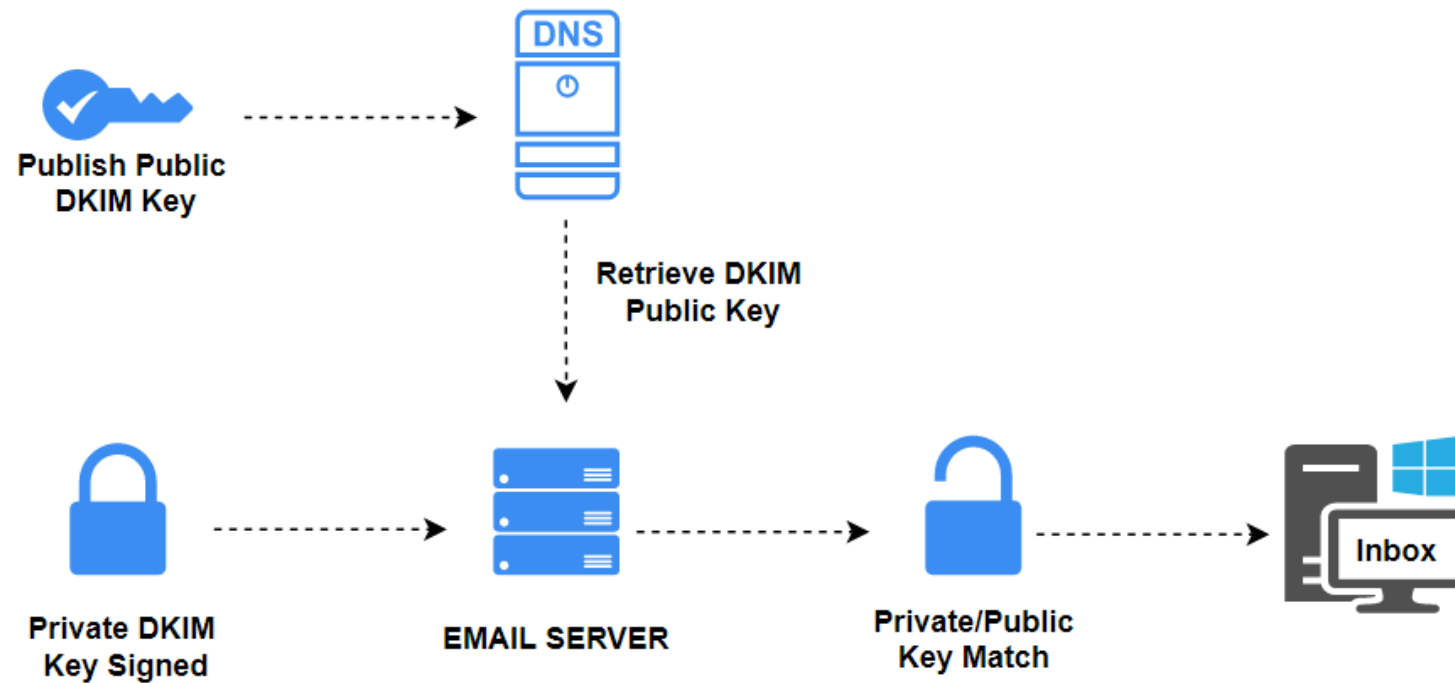


Each SPF record allows for 10 DNS lookups. If your SPF record exceeds this limit, receiving servers automatically fail SPF authentication

# Email Authentication protocols

## DKIM

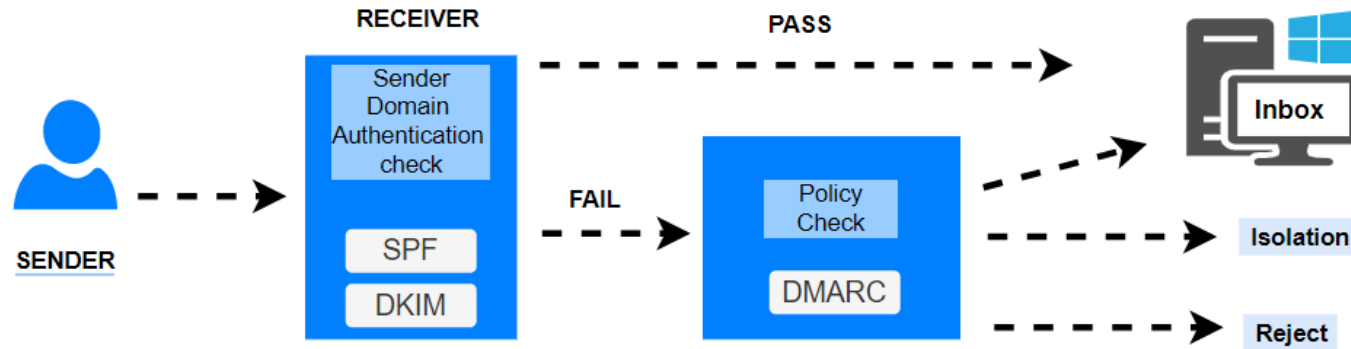
---





# Email Authentication protocols

## DMARC



# Email Header Inspection

A thin, vertical blue line is positioned to the right of the text, extending from the top of the word 'Header' down to the bottom of the word 'Inspection'.

# Email Header Inspection

```
1 Primit: din [REDACTED]
2 de atlas312.free.mail.bf1.yahoo.com cu HTTPS; Duminică, 2 ianuarie 2022 14:55:14 +0000
3 Cale de intoarcere: [REDACTED].com>
4 Ip de origine X: [66.163.185.58]
5 Primit-SPF: trece (domeniul yahoo.com desemnează 66.163.185.58 ca expeditor permis)
6 Autentificare-Rezultate: atlas312.free.mail.bf1.yahoo.com;
  dkim=pass header.i=@yahoo.com header.s=s2048;
  spf=pass smtp.mailfrom=yahoo.com;
  dmarc=pass (p=RESPING) header.from=yahoo.com;
7 X-Aparent-Către: [REDACTED].com; Duminică, 2 ianuarie 2022 14:55:14 +0000
8 Primit: de la 66.163.185.58 (EHLO sonic313-35.consmr.mail.nel.yahoo.com)
9 până la [REDACTED] cu SMTP-uri
10 (versiunea=TLS1_2 cipher=TLS ECDHE_RSA WITH_AES_128_GCM_SHA256);
11 Duminică, 02 ianuarie 2022 14:55:14 +0000
12 Semnătura DKIM: v=1; a=rsa-sha256; c=relaxat/relaxat; d=yahoo.com; s=s2048; t=1641135314; bh=hFEL1SRXu/tWgXayiWs74QJPBjmb2Pc94gnRiR8Z2dw=; h=Data:From:Subject:
13 X-SONIC-DKIM-SIGN: v=1; a=rsa-sha256; c=relaxat/relaxat; d=yahoo.com; s=s2048; t=1641135314; bh=gONfvzqylen78FaDo/AroI4RTfMjyHlXEotS1MyQGtZ=; h=X-Sonic-MF:Data:
14
15 Primit: de la sonic.gate.mail.nel.yahoo.com de către sonic313.consmr.mail.nel.yahoo.com cu HTTP; Duminică, 2 ianuarie 2022 14:55:14 +0000
16 Primit: de kubenode538.mail-prod1.omega.bf1.yahoo.com (VZM Hermes SMTP Server) cu ID-ul ESMTPA 72cf9863b9d498d56dfea14480754dae;
17 Duminică, 02 ianuarie 2022 14:53:13 +0000 (UTC)
18
19 Tip de conținut: mai multe părți/alternativ;
20 boundary="-----qES5dXcbeFYCs3fzFOArfMu"
21 ID-ul mesajului: <1999c398-6076-e731-6415-c8166024c261@yahoo.com>
22 Data: duminica, 2 ianuarie 2022 15:52:42 +0100
23 Versiunea MIME: 1.0
24 Agent utilizator: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:91.0) Gecko/20100101
25 Thunderbird/91.4.1
26 Limbă de conținut: ro-US
27 De la: Yahoo Security! <[REDACTED].com>
28 Subiect: *** ADVERTISMENT FINAL: EMAILUL DVS. SE VA ÎNCHIDE ÎN 24 DE ORE ***
29 Către: destinatari-nedezvăluți;
30 Referințe: <1999c398-6076-e731-6415-c8166024c261.ref@yahoo.com>
31 X-Mailer: WebService/1.1.19551 mail.backend.jedi.jws.acl:role.jedi.acl.token.atz.jws.hermes.yahoo
32 Lungimea conținutului: 16466
33
34 Acesta este un mesaj cu mai multe părți în format MIME.
35 -----qES5dXcbeFYCs3fzFOArfMu
36 Content-Type: text/plain; set de caractere=UTF-8; format=curgere
37 Codare de transfer de conținut: 8 biți
38
39
40
41 *Stimate utilizator,*
42 Contul a expirat
43 E-mailul dvs. va fi închis la 01.02.2022
44 Stimat utilizator
45
46 Â Actualizați-vă? contul
47 Actualizați-vă contul <https://tinyurl.com/[REDACTED]>
```

# Email Content Inspection

A thin, vertical blue line is positioned to the right of the text, extending from the top of the word 'Inspection' down to the bottom of the word 'Content'.

# Red Flags

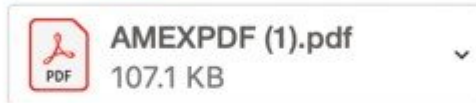
## Important Message From American Express



 **American Express** <admin@americanexpress-supportcenter.ml>

Monday, April 8, 2019 at 7:13 AM

[Show Details](#)



[Download All](#)



[Preview All](#)

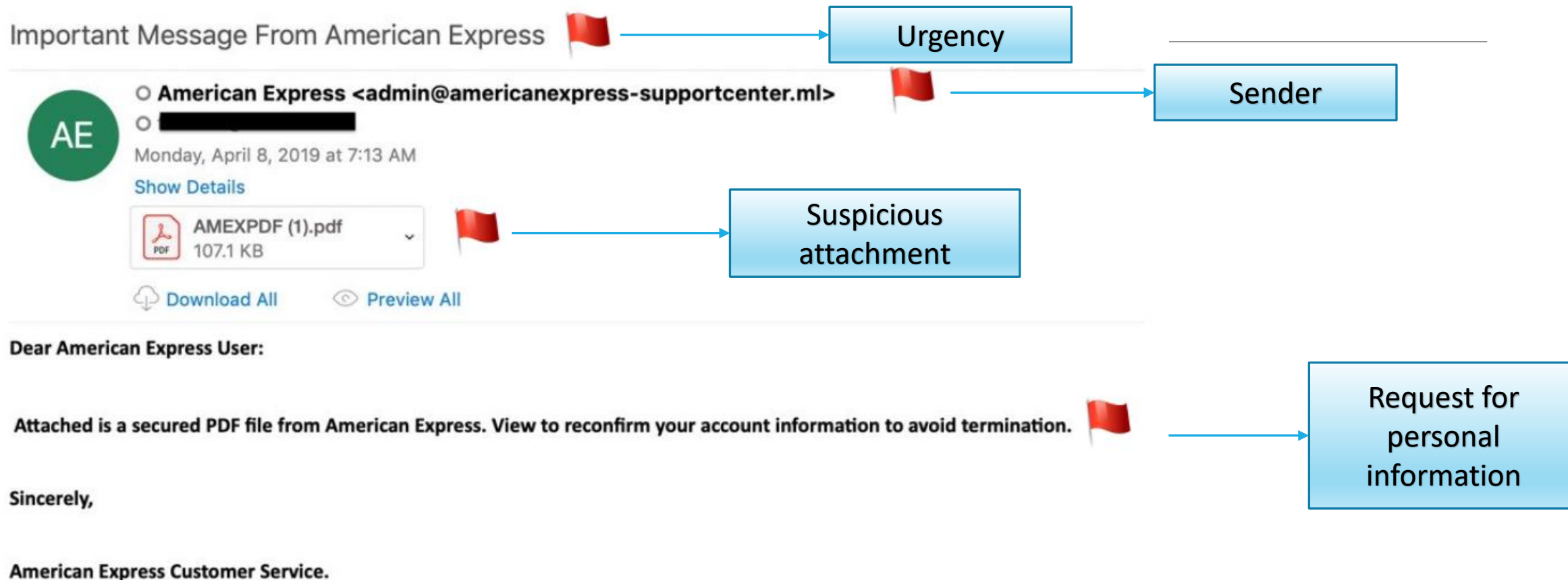
**Dear American Express User:**

**Attached is a secured PDF file from American Express. View to reconfirm your account information to avoid termination.**

**Sincerely,**

**American Express Customer Service.**

# Red Flags



# Red Flags

De la: "Yahoo Security!" [REDACTED]

Către: indisponibil

Cc:

Trimis: dum., ian. 2, 2022 la 16:55

Subiect: \*\*\* FINAL WARNING: YOUR E-MAIL WILL CLOSE WITHIN 24 HOURS \*\*\*

Dear User,

## Account expired

Your email will be closed at 01/02/2022

Stimate utilizator

Acest mesaj vă este trimis pentru a vă informa că contul dumneavoastră va expira la 01/02/2022

Dacă doriți să continuați să utilizați acest cont, vă rugăm să faceți upgrade la serviciile noastre. Ignorarea acestui mesaj va determina închiderea contului

Actualizați-vă contul

[Update your account](#)

Thank you,  
Mail Team ©2021

# Red Flags

De la: "Yahoo Security!" [REDACTED]

Către: indisponibil

Cc:

Trimis: dum., ian. 2, 2022 la 16:55

Subject: \*\*\* FINAL WARNING: YOUR E-MAIL WILL CLOSE WITHIN 24 HOURS \*\*\*



Urgency

Dear User,

## Account expired

Your email will be closed at 01/02/2022

Stimate utilizator

Acest mesaj vă este trimis pentru a vă informa că contul dumneavoastră va expira la 01/02/2022



Bad Language

Dacă doriți să continuați să utilizați acest cont, vă rugăm să faceți upgrade la serviciile noastre. Ignorarea acestui mesaj va determina închiderea contului

Actualizați-vă contul

[Update your account](#)



Embedded URL

Thank you,  
Mail Team ©2021




# URL investigation



# URL Investigation



## OSINT

 Features | Pricing | Live API | About Us | Sign In | Sign Up

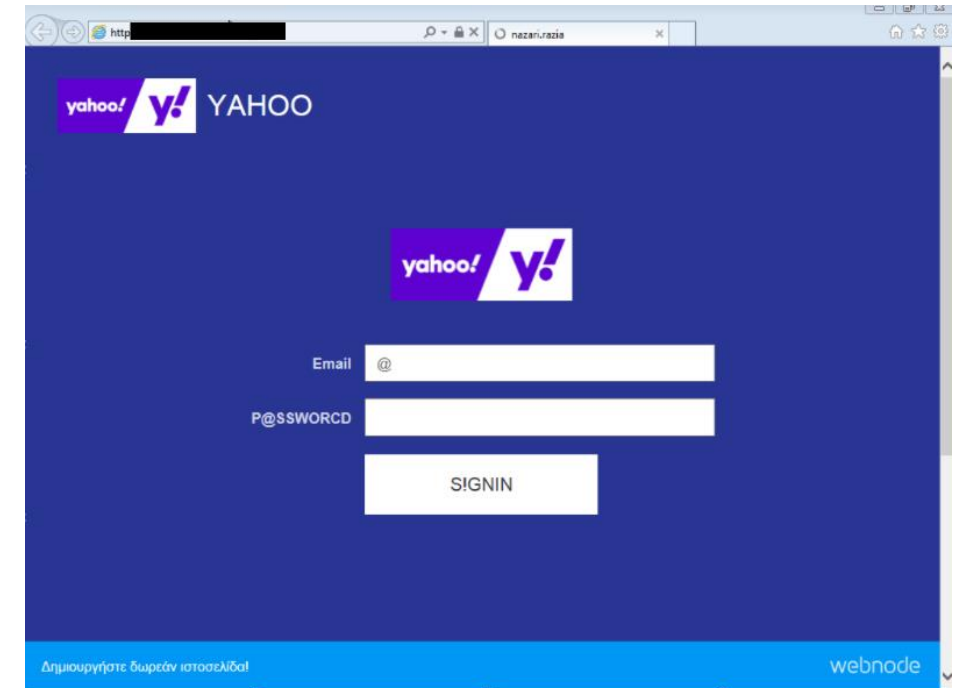
---

Online cross-browser testing

**Test now!**

 Windows 7 |  Internet Explorer | 11

Get a browser and start testing in 5 seconds!



# URL Investigation

## OSINT



File/URL File Collection Report Search YARA Search String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.

Drag & Drop For Instant Analysis

or

[Analyze](#)



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE URL SEARCH


Search or scan a URL

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)

Want to automate submissions? [Check our API](#), free quota grants available for new file uploads

# URL Investigation

## OSINT


[urlscan.io](#)[Home](#)[Search](#)[Live](#)[API](#)[Blog](#)[Docs](#)[Pricing](#)[Login](#)





Sponsored by  
**SecurityTrails**

# urlscan.io

*A sandbox for the web*

[▶ Public Scan](#)[⚙ Options](#)

Recent scans  Updates every 10s - Last update: 13:44:02

 URL	Age	Size	 IPs		
---	-----	------	---	---	---

# Suspicious Attachment Investigation

OLETOOLS –  
DOC, DOCX, XLS

# Suspicious Attachment Investigation

## Installing OLE-TOOLS

---

- Get Python3  
<https://www.python.org/downloads/windows/>
- Install pip: *python get-pip.py* (cmd command)
- Install oletools: *pip install -U oletools* (cmd command)

Windows



- `sudo apt install python3.8`
- `sudo apt install python3-pip`
- `sudo -H pip install -U oletools`

Ubuntu



# Suspicious Attachment Investigation

## OLE-TOOLS - olemeta

- Document Metadata and standard properties

```
(kali㉿kali)-[~/Desktop/Curs12]
$ olemeta sample2.docx
olemeta 0.54 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

FILE: sample2.docx

Properties from the SummaryInformation stream:
+-----+-----+
|Property|Value|
+-----+-----+
|codepage|1252|
|author|admin|
|template|Normal.dotm|
|last_saved_by|oplu|
|revision_number|3|
|total_edit_time|60|
|create_time|2022-01-05 22:52:00|
|last_saved_time|2022-01-05 22:53:00|
|num_pages|1|
|num_words|0|
|num_chars|1|
|creating_application|Microsoft Office Word|
|security|0|
+-----+-----+
```

```
Properties from the DocumentSummaryInformation stream:
+-----+-----+
|Property|Value|
+-----+-----+
|codepage_doc|1252|
|lines|1|
|paragraphs|1|
|scale_crop|False|
|company|
|links_dirty|False|
|chars_with_spaces|1|
|shared_doc|False|
|hlinks_changed|False|
|version|917504|
+-----+-----+
```

# Suspicious Attachment Investigation

## OLE-TOOLS - oleid

```
(kali㉿kali)~[~/Desktop/Curs12]
$ oleid sample2.docx
oleid 0.60.dev1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: sample2.docx
```

Indicator	Value	Risk	Description
File format	MS Word 97-2003 Document or Template	info	
Container format	OLE	info	Container type
Application name	Microsoft Office Word	info	Application name declared in properties
Properties code page	1252: ANSI Latin 1; Western European (Windows)	info	Code page used for properties
Author	admin	info	Author declared in properties
Encrypted	False	none	The file is not encrypted
VBA Macros	Yes, suspicious	HIGH	This file contains VBA macros. Suspicious keywords were found. Use olevba and mraptor for more info.
XLM Macros	No	none	This file does not contain Excel 4/XLM macros.
External Relationships	0	none	External relationships such as remote templates, remote OLE objects, etc



File Contains Macros



# Suspicious Attachment Investigation

## OLE-TOOLS – olevba

- Extracting Macros with olevba

```
(kali㉿kali)-[~/Desktop/Curs12]
$ olevba sample2.docx
olevba 0.60 on Python 3.9.2 - http://decalage.info/python/oletools

FILE: sample2.docx
Type: OLE

VBA MACRO ThisDocument.cls
in file: sample2.docx - OLE stream: 'Macros/VBA/ThisDocument'
-----
Sub OYwrUVCJckZuLvRBMSOZrFN()

Dim tudfTFyTfytdDfUDTYfUuHIUgKJGhGftfyRftfFrfrTRFtrydeTeStsSerSYDdtYdFYygOuiyguFdfrdDuFFtdt As String
Dim feuxAsQgYIrtNqvIFoBOJnYGUHJvGRERwseDGHFvVJFddHCfDdFCGhDCFHDGGESdRFgjHgkghGfdhgsFwsgdxHFCGvgJfGKuyiJhFDHfCJGVJhgvcgFCsDhfHfgdhfccg As String
Dim GFNCfbxbvcbCKXzSyWoOoAKIHUjHGHGFDhFdFsDXgDSChnFGkhHgfhDESrCVGBhBgFdrgrdFGKJGFDGsXDSXSzSFDzgdxcFhvJGvgJJKHGfCchFGcgdfcFGCFXDdbcfBfcVNgjvvh As String
Dim FABzEqwDUvuKADuTwcZHIHKjhJgmNHGFCfDSFWSXDGXgcfHVGhvhFhKJHkIHHGFHDgrdErSDgrXRfrGDchtvJyUBMJGtfHDFrJFtYGYKUUGgYJtfdTRjHdrgfdchDXdgXfsESgeDhJGygKj As String
Dim JTHFgnwQGxLVEErrSboPkOnEQFCwIjkjHBgHBhgvhFGCFCDXrdReSwaqsewsawzxSezXftcDtFdRdfThfgffchfgHGfGjhGvhggdGCGcgFFCVJHHGVUhhkGFBdFXcg As String
Dim OLirDjfqHIegpMtWnTZOIjkjHUjbBhGgtfGTRDreeSWSeXTRXcGCdCfghvBJNJIHgGtfyYfYkuYTftFyfthfDghcGFCxDSDXgSDhfgVhKJHGfvmhBjoPIuohbhgcHG As String
feuxAsQgYIrtNqvIFoBOJnYGUHJvGRERwseDGHFvVJFddHCfDdFCGhDCFHDGGESdRFgjHgkghGfdhgsFwsgdxHFCGvgJfGKuyiJhFDHfCJGVJhgvcgFCsDhfHfgdhfccg = Decrypt("fyf/dsdd")
GFNCfbxbvcbCKXzSyWoOoAKIHUjHGHGFDhFdFsDXgDSChnFGkhHgfhDESrCVGBhBgFdrgrdFGKJGFDGsXDSXSzSFDzgdxcFhvJGvgJJKHGfCchFGcgdfcFGCFXDdbcfBfcVNgjvvh = Environ$("AppData") & "\" & feuxAsQgYIrtNqvI
YGUHJvGRERwseDGHFvVJFddHCfDdFCGhDCFHDGGESdRFgjHgkghGfdhgsFwsgdxHFCGvgJfGKuyiJhFDHfCJGVJhgvcgFCsDhfHfgdhfccg
```

# Suspicious Attachment Investigation

PDFID

# Suspicious Attachment Investigation

pdfid

```
(kali㉿kali)-[~/Desktop/Curs12]
```

```
$ pdfid sample3.pdf
```

```
PDFiD 0.2.8 sample3.pdf
```

```
PDF Header: %PDF-1.4
```

obj	56
endobj	56
stream	21
endstream	21
xref	2
trailer	2
startxref	2
/Page	7
/Encrypt	0
/ObjStm	0
/JS	1
/JavaScript	2
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0
/XFA	0
/Colors > 2^24	0



Embedded Script

# Resources

---

python <https://www.python.org/downloads/release/python-380/>

oletools <https://pypi.org/project/oletools/0.04/>

pdftools <https://pypi.org/project/pdftools/>

VirusTotal <https://www.virustotal.com/gui/>

HybridAnalysis <https://www.hybrid-analysis.com/>

URLscan <https://urlscan.io/>

Browserling <https://www.browserling.com/>

Thank you!