Antiphishing ed oltre: la protezione del brand e del dominio di posta

HACK IN BO Winter 2022 Edition
1g^a EDIZIONE

Raffaele Colavecchi
Com.Tel S.p.A.

Raffaele.Colavecchi@comtelitalia.it

Blog: https://www.cloudcommunity.it

LinkedIN Group: **DMARC Italia**
https://www.linkedin.com/groups/12726326/

Agenda

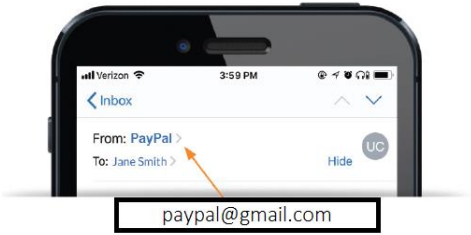
- ➔ Il Phishing via email
- ➔ Cos’è il DMARC?
- ➔ La ciliegina sulla torta
- ➔ Domande e Risposte
- ➔ Casi Reali
- ➔ Conclusioni

75%

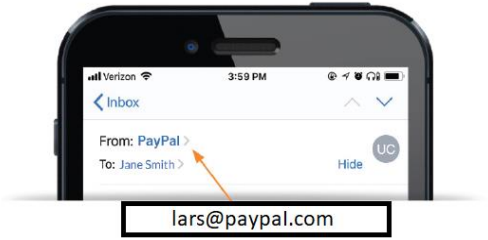
dei cyber-attacchi cominciano con una email.

Diversi tipi di attacchi phishing

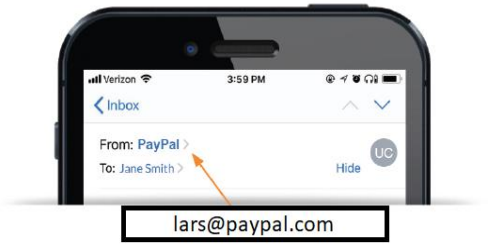
- **Display Name Spoofing (FROM NAME)**
  paypal@gmail.com



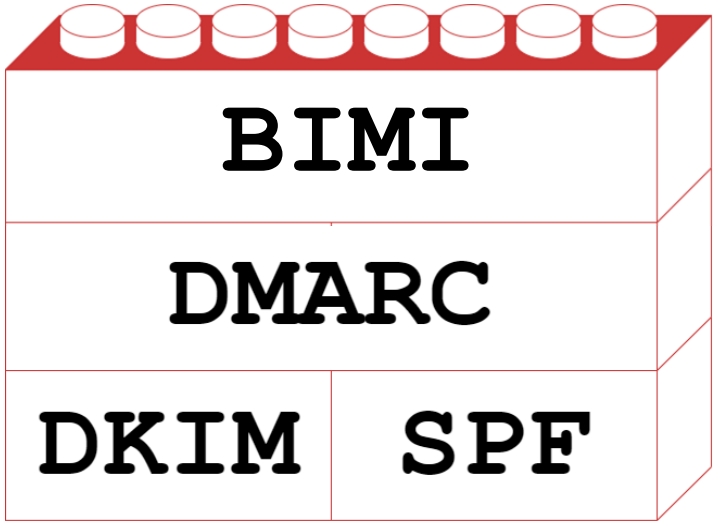
- **Simil Domain**
  lars@paypaI.com – la lettera l di paypal.com
  è la lettera i maiuscola al posto della lettera L



- **Domain Name Spoofing (FROM EMAIL)**
  lars@paypal.com – Il dominio non è protetto con DMARC



Cos’è il DMARC?



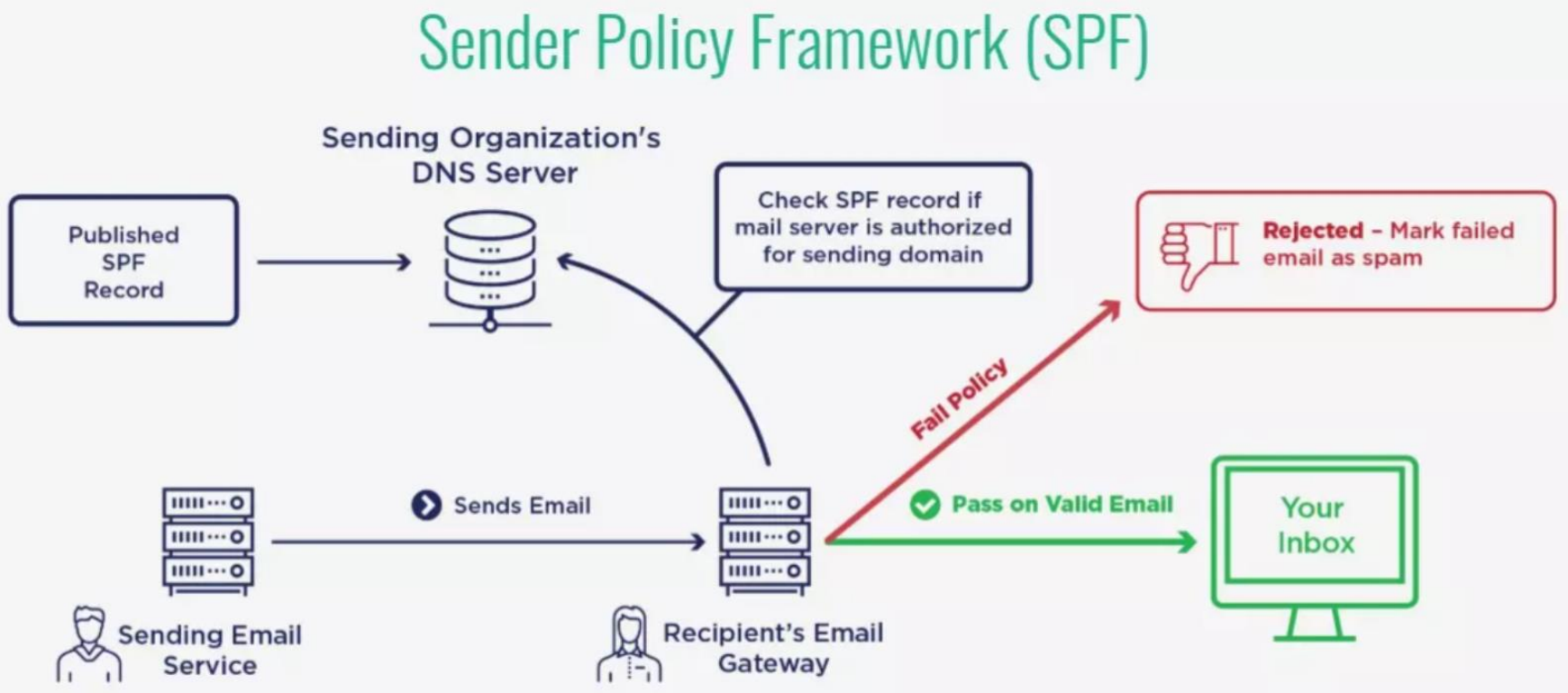
← La ciliegina sulla torta

← L’evoluzione

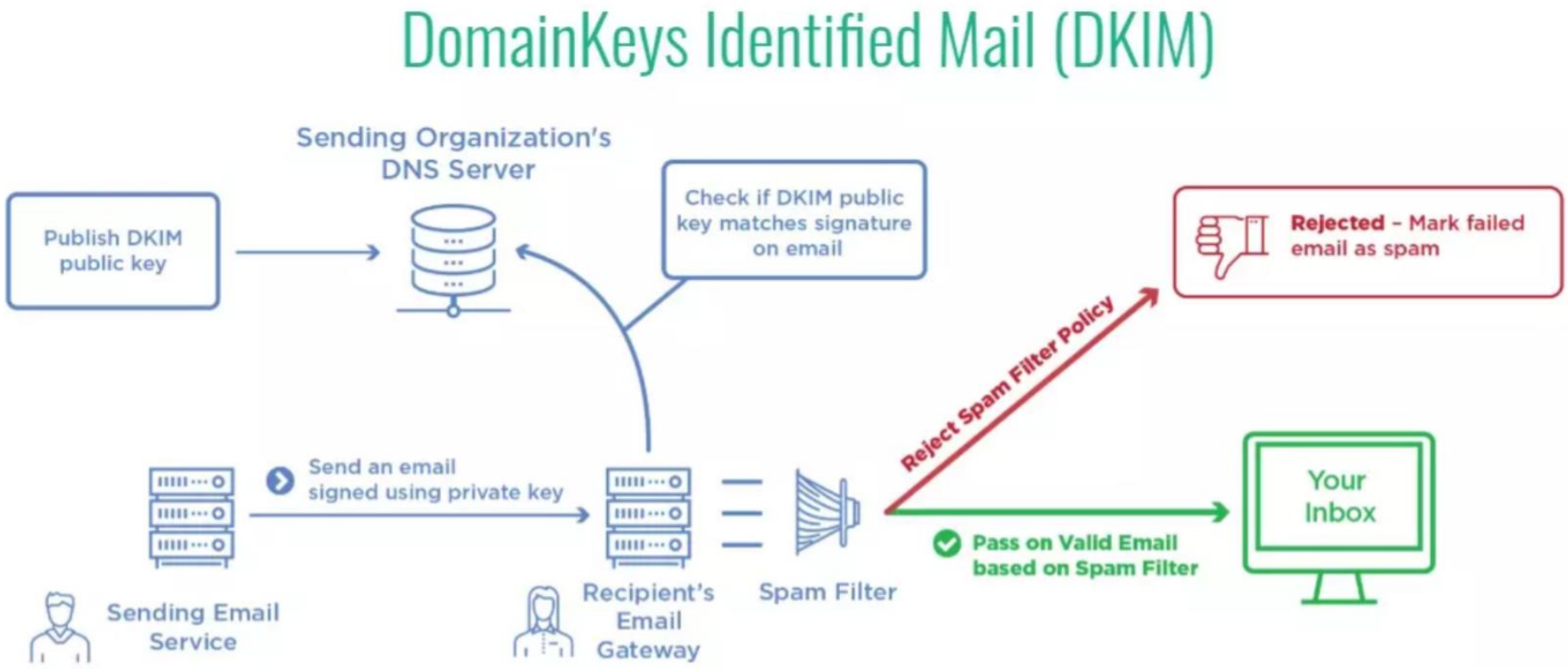
← Le basi

Non sono prodotti ma protocolli basati sul DNS

Il protocollo SPF



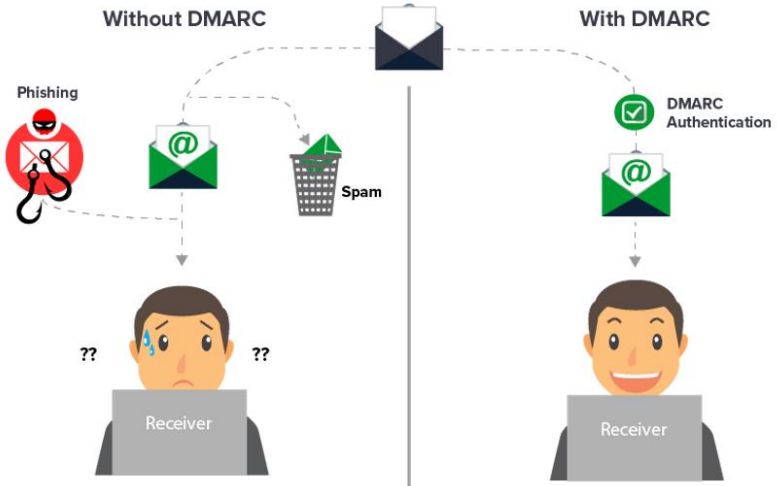
Il protocollo DKIM



Domain Name Spoofing (FROM EMAIL)

Envelope	HELO mailserver.dominioSPF.com Mail From: utente@dominioSPF.com ← Controllo SPF (Return-Path) Rcpt To: malcapitato@dominioDestinatario.it DATA
Body	From: CEO <ceo@dominioSenzaDMARC.it> ← Mittente visualizzato To: Nome Cognome <malcapitato@dominioDestinatario.it> Subject: Cambio IBAN per pagamento fattura Date: Sab, 3 Dic 2022 08:54:23 +0100 (UTC) Message-ID: <20221203085423.96CD64A610@dominioSPF.com> Gentile Malcapitato, Allego il nuovo IBAN per il pagamento della fattura Il CEO del tuo fornitore preferito Firma DKIM applicabile con qualsiasi dominio (in genere il provider di posta)

Possiamo vivere nell'incertezza?



Nessun controllo sull'uso del dominio di posta
Dominio di posta impersonificabile (phishing)
Danno d'immagine

Massimo controllo sull'uso del dominio di posta
Email fasulle rigettate
Dominio di posta "autenticato"

Il dominio di posta è un asset aziendale

Perchè implementare il DMARC

HACK IN BO
Winter 2022 Edition
19ª EDIZIONE

- Allineamento tra il dominio SPF/DKIM ed il dominio From
- Indicazione al destinatario su come trattare le email
- Indicazione al destinatario sul feedback delle email ricevute
- Indicazione al destinatario su tematiche forensi
- Massima tutela della privacy dei mittenti e destinatari
- Massima protezione dei domini acquistati e non utilizzati
- Implementato da tutti i maggiori provider di posta
- Implementato da tutti i maggiori fornitori di servizi antispam

La protezione del brand – La policy DMARC

p=none

Monitoraggio. Nessun impatto sul flusso di posta. **Si parte da qui**.

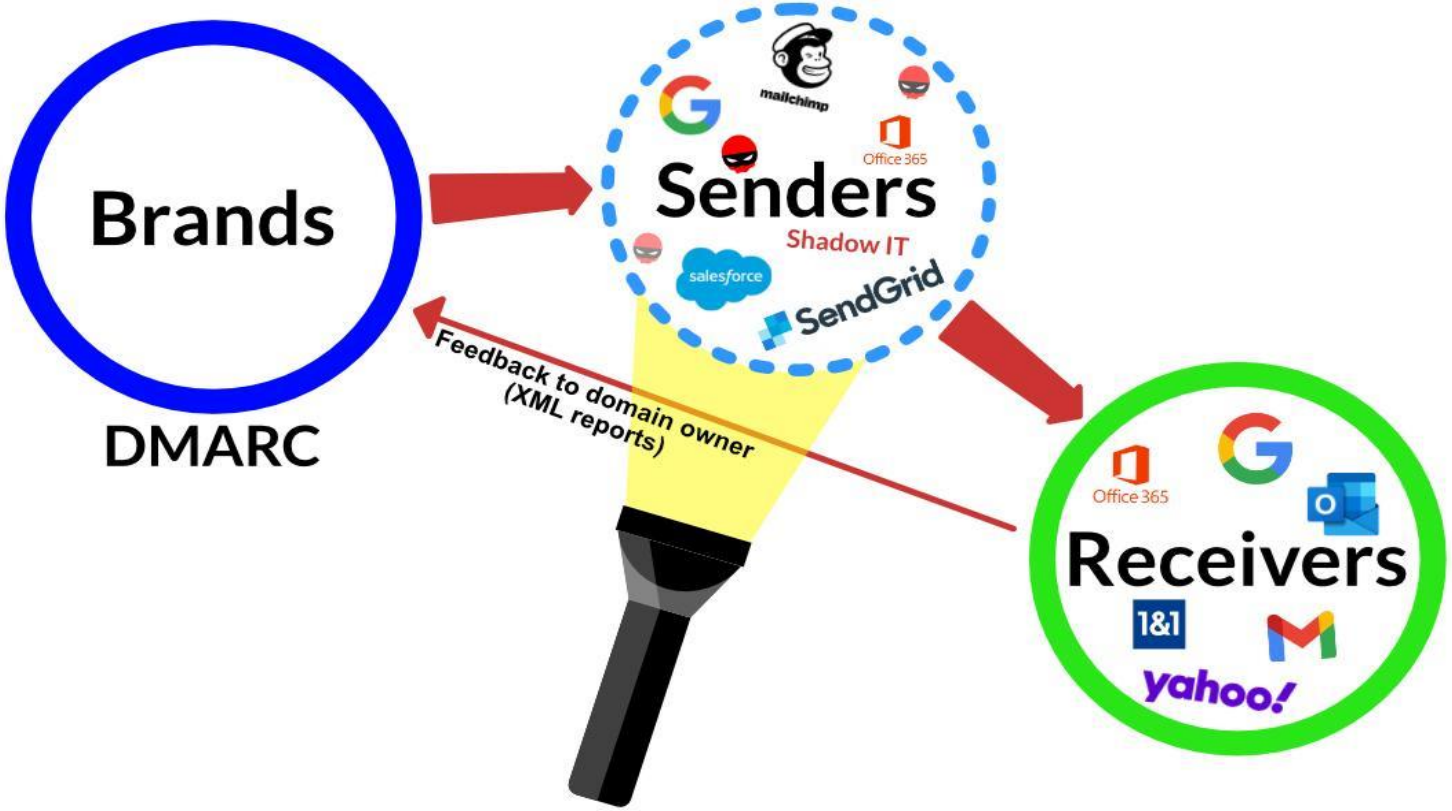
p=quarantine

Quarantena. Le email che non rispettano il protocollo SPF o DKIM vengono quarantenate dal destinatario. **Primo passaggio importante**.

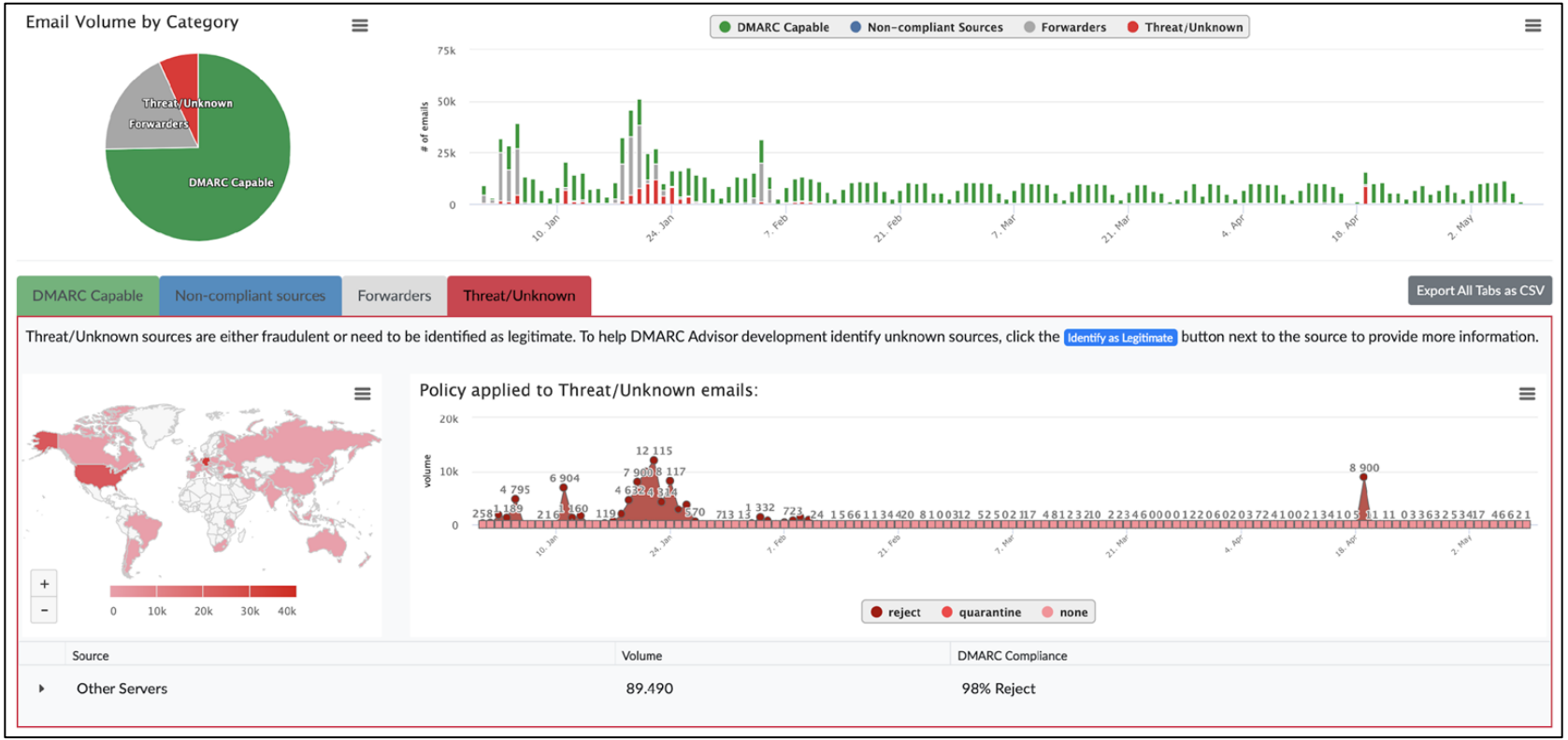
p=reject

Blocco. Le email che non rispettano i controlli DMARC vengono rigettate dal destinatario. **Fase finale**.

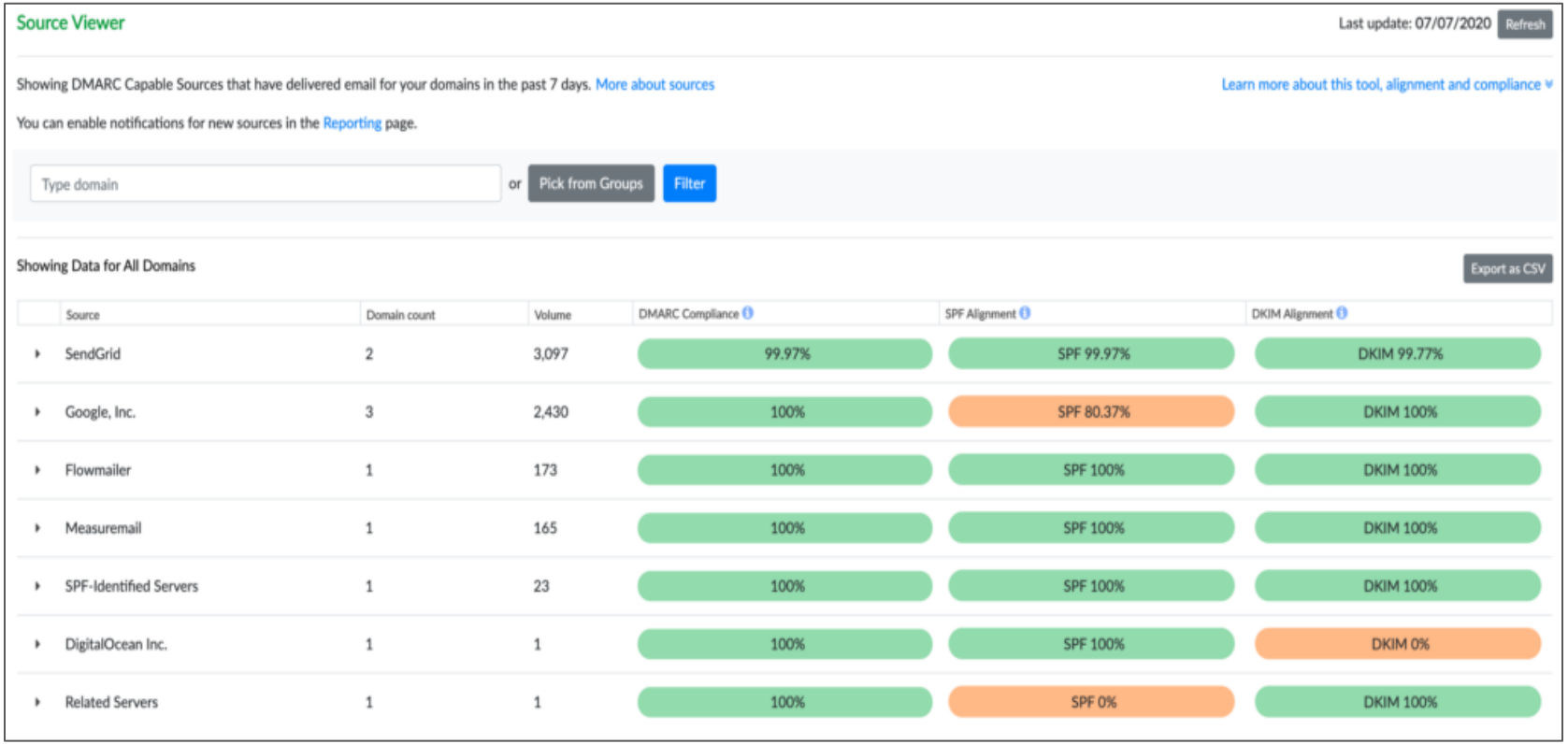
L’importanza della reportistica



Chi usa il mio dominio per attaccare?



Quali sono le mie fonti di spedizione?



Source Viewer

Last update: 07/07/2020 Refresh

Showing DMARC Capable Sources that have delivered email for your domains in the past 7 days. More about sources

Learn more about this tool, alignment and compliance

You can enable notifications for new sources in the Reporting page.

Type domain or Pick from Groups Filter

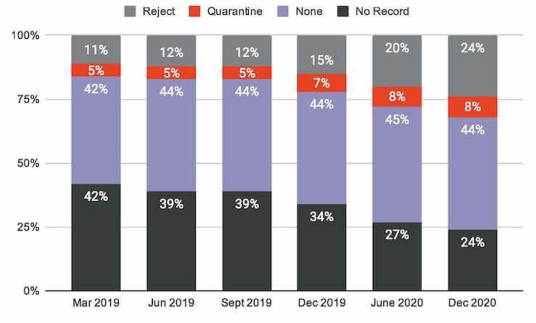
Showing Data for All Domains

Export as CSV

Source	Domain count	Volume	DMARC Compliance	SPF Alignment	DKIM Alignment
SendGrid	2	3,097	99.97%	SPF 99.97%	DKIM 99.77%
Google, Inc.	3	2,430	100%	SPF 80.37%	DKIM 100%
Flowmailer	1	173	100%	SPF 100%	DKIM 100%
Measuremail	1	165	100%	SPF 100%	DKIM 100%
SPF-Identified Servers	1	23	100%	SPF 100%	DKIM 100%
DigitalOcean Inc.	1	1	100%	SPF 100%	DKIM 0%
Related Servers	1	1	100%	SPF 0%	DKIM 100%

Esempi di configurazione DMARC

Record TXT _dmarc.dominio.it

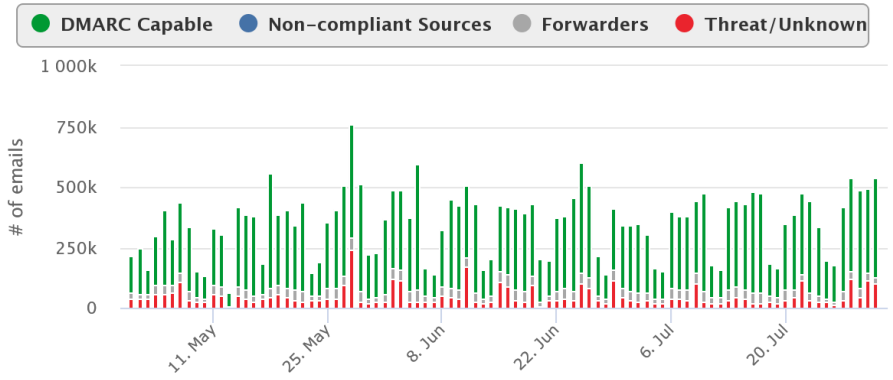


- **L'ignorante** NON PRESENTE
- **L'informato** v=DMARC1; p=none
- **Il lettore di bit** v=DMARC1; p=none; rua=mailto:dmarc@dominio.it
- **Il lavoratore** v=DMARC1; p=quarantine; rua=mailto:cliente@RepDMARCxxx.com; ruf=mailto: cliente@RepDMARCxxx.com
- **Il sicuro** v=DMARC1; p=reject
- **Il saggio** v=DMARC1; p=reject; rua=mailto:cliente@RepDMARCxxx.com; ruf=mailto: cliente@RepDMARCxxx.com

L’impatto di una policy di blocco

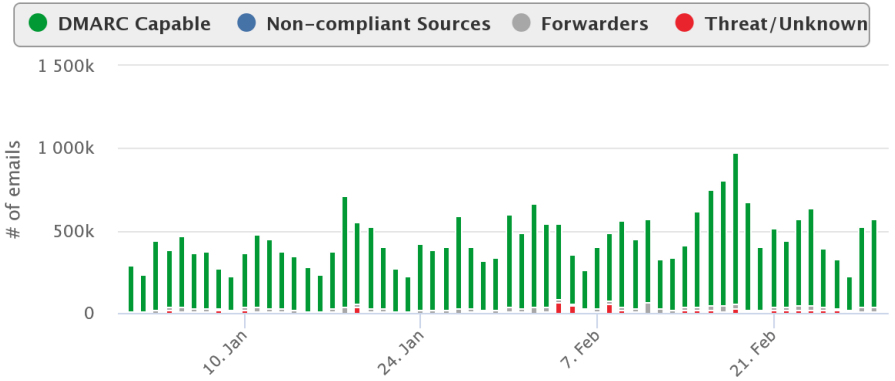
HACK IN BO Winter 2022 Edition 1ª EDIZIONE

Prima (appena aggiunto il primo record DMARC)



Threat Volume	DMARC policy
4.386.392	Monitoraggio (p=none)

Dopo (implementazione terminata e dominio protetto)



Threat Volume	DMARC policy
1.708.885	Blocco (p=reject)

La ciliegina sulla torta – Il BIMI

- ➔ **Il logo aziendale nelle tue email verso clienti e fornitori**
- ➔ **Con DMARC policy p=quarantine o p=reject**

Supports BIMI

Apple Mail / iCloud Mail

* Available in MacOS/iOS16. Expected in Fall 2022.

Fastmail

Pobox

Google Gmail Google Workspace

yahoo! Aol. Netscape

Considering BIMI

BT

COMCAST

LA POSTE

QUALITIA

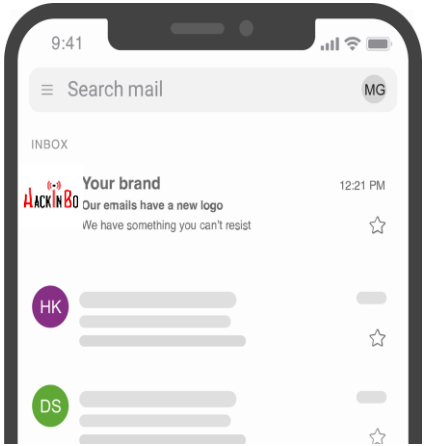
SEZNAM.CZ

WEB.DE GMX

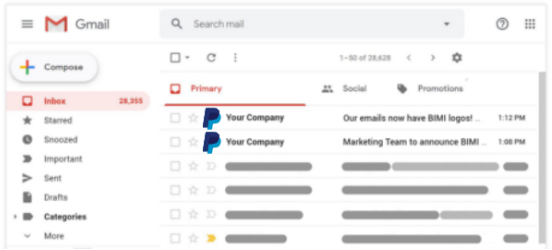
YAHOO! JAPAN

Does not support BIMI

Microsoft Outlook Office 365



bimi:paypal.com | Solve Email Delivery Problems | bimi




```
v=BIMI1; l=https://www.paypalobjects.com/marketing/web/logos/paypal.svg; a=https://www.paypalobjects.com/marketing/web/logos/pay
```

Tag	TagValue	Name	Description
v	BIMI1	Version	Identifies the record retrieved as a BIMI record. It must be the first tag in the record.
l	https://www.paypalobjects.com/marketing/web/logos/paypal.svg	Locations	Comma separated list of base URLs representing the location of the brand indicator files.
a	https://www.paypalobjects.com/marketing/web/logos/paypal_com.pem	Trust Authorities	Optional Validation Information for verifying bimi locations.

Esempio 1 – Caso comune di attacco

Header Name	Header Value
Authentication-Results	spf=softfail (sender IP is 79.60.226.174) smtp.mailfrom=netsearch.org; dkim=none (message not signed) header.d=none;dmarc=none action=none header.from=azienda.it
Received-SPF	SoftFail (protection.outlook.com: domain of transitioning netsearch.org discourages use of 79.60.226.174 as permitted sender)
To	amministrazione@comtelitalia.it
Subject	Ricevuta di pagamento - Transazione n. 202210357150476302
Reply-To	ricevuta-pagaonline@azienda.it
From	ricevuta-pagaonline@azienda.it
Message-ID	<fd8c666f-b8da33f51-71ee-21f0ba61e0b7@LYGIDED.PUXOXED.netsearch.org>
Date	Mon, 24 Oct 2022 11:54:07 +0100
Return-Path	fpmdrccyh@netsearch.org

Esempio 2 – Spoofing con DKIM

Header Name	Header Value
Authentication-Results	spf=pass (sender IP is 168.245.59.205) smtp.mailfrom=sendgrid.net; dkim=pass (signature was verified) header.d=sendgrid.net;dmarc=fail action=none header.from=mail.com
Received-SPF	Pass (protection.outlook.com: domain of sendgrid.net designates 168.245.59.205 as permitted sender) receiver=protection.outlook.com; client-ip=168.245.59.205; helo=xvfrpbcd.outbound-mail.sendgrid.net; pr=C
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=sendgrid.net; h=content-type:from:mime-version:subject:reply-to:to:list-unsubscribe: cc; s=smtpapi; bh=g3AzA/RVjLbt5YPtF7b…..
To	marketing@comtelitalia.it
Date	Mon, 14 Nov 2022 08:48:27 +0000 (UTC)
From	SERVER <it0000reply@mail.com>
Message-ID	<cyG_3Gy6S0u_DuEJAEsrpg@geopod-ismtpd-1-1>
Subject	Avviso: la tua casella di posta piena
Reply-To	it0000reply@mail.com
Return-Path	bounces+29955092-f6a3-marketing=comtelitalia.it@sendgrid.net

Esempio 3 – Mail completamente falsa

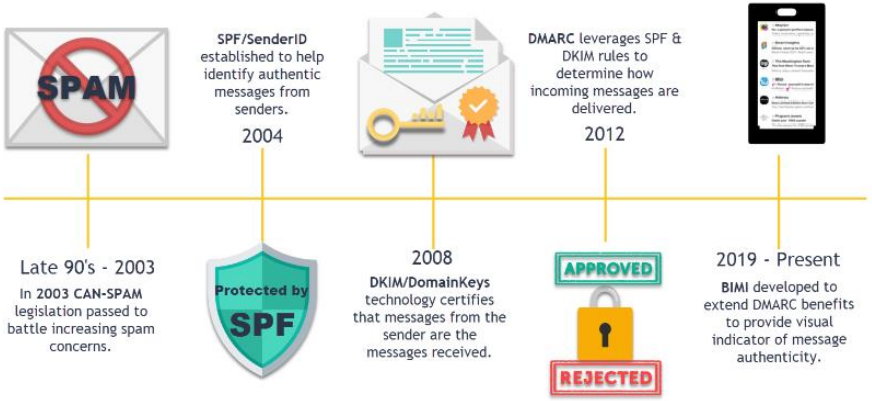
Header Name	Header Value
Authentication-Results	spf=fail (sender IP is 217.61.208.245) smtp.mailfrom=censored.it; dkim=none (message not signed) header.d=none;dmarc=fail action=none header.from=censored.it
Received-SPF	Fail (protection.outlook.com: domain of censored.it does not designate 217.61.208.245 as permitted sender) receiver=protection.outlook.com; client-ip=217.61.208.245; helo=hostingoedim.loading.net;
Date	Thu, 10 Nov 2022 09:00:22 +0100
From	CENSORED <e-mailbox@censored.it>
To	undisclosed-recipients:;
Subject	Pagamento tramite bonifico bancario
Message-ID	<58606a7cbbed82973f6b80e0d6e94906@censored.it>
Return-Path	e-cdp@censored.it

Esempio 4 – Attacco sventato

Header Name	Header Value
Authentication-Results	spf=pass (sender IP is 103.253.125.162) smtp.mailfrom=britishpaints.co.in; dkim=none (message not signed) header.d=none;dmarc=fail action=oreject header.from=comtelitalia.it
Received-SPF	Pass (protection.outlook.com: domain of britishpaints.co.in designates 103.253.125.162 as permitted sender) receiver=protection.outlook.com; client-ip=103.253.125.162; helo=mail.britishpaints.co.in; pr=C
Reply-To	"comtelitalia.it" <host@comtelitalia.it>
From	"comtelitalia.it" <host@comtelitalia.it>
To	marketing@comtelitalia.it
Subject	Last warning! You have 6 Incoming Messages Blocked!
Date	10 Nov 2022 06:19:42 +0000
Message-ID	<20221110061942.DF8BFBDBBF963EEE@comtelitalia.it>
Return-Path	terr01.kot@britishpaints.co.in

Conclusioni

- L'email la usano TUTTI
- Se sei piccolo, il DMARC è abbastanza facile, se sei grande NO



- Il tuo antivirus e antispam proteggono te, non l'uso del tuo dominio in attacchi nei confronti di CLIENTI e FORNITORI
- Avere le caselle di posta su grandi provider NON implica l'implementazione automatica del DMARC

Grazie per l’attenzione

Raffaele Colavecchi

Com.Tel S.p.A.

Raffaele.Colavecchi@comtelitalia.it

Blog: https://www.cloudcommunity.it

LinkedIN Group: **DMARC Italia**
https://www.linkedin.com/groups/12726326/