DEFENDIENDO LA REPUTACIÓN DE TUS DIRECCIONES IP: ABUSE, SPAM Y LISTAS NEGRAS

Jorge Varela / CEO TRUXGO

Las blacklists de IP son listas utilizadas para identificar y bloquear direcciones IP que se consideran maliciosas, sospechosas o no deseadas.

TRUXGO

Tipos de Blacklist

- Blacklists públicas.
- Blacklists privadas.
- Blacklists de correo electrónico (RBL).
- Blacklists geográficas.
- Blacklists dinámicas.
- Blacklists basadas en reputación.

SPAMHAUS

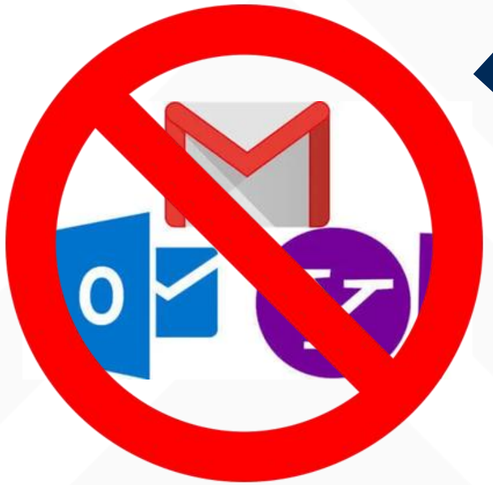
TALOS
CISCO

Barracuda

abusix

SpamRATS!
(Really Annoying Trouble Spots)

spamcop.net



CloudLock

AbuseIPDB

UCEPROTECT-NETWORK

TRUXGO

BLACKLIST

TRUXGO

[redacted] was found in our database!

This IP was reported **457** times. Confidence of Abuse is **100%**: ?

100%

ISP [redacted]

Usage Type Search Engine Spider

Domain Name [redacted]

Country [redacted]

City [redacted]

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT [redacted]

WHOIS [redacted]

TRUXGO

Reporter	Date	Comment	Categories
✔ 1000grad.com	1 minute ago	5x Failed Password	Brute-Force SSH
✔ woutvde	5 hours ago		Brute-Force SSH
✔ InfinitzHost	5 hours ago	Unauthorized connection attempt detected from IP add ress [redacted] to port 22 [V]	Brute-Force Exploited Host
✔ HyperSpeed	5 hours ago	Jul 4 13:17:02 NY2 sshd[3129620]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid= ... show more	Brute-Force SSH
✔ Parth Maniar	5 hours ago	SSH login attempts (SSH bruteforce attack). For more i nformation, or to report interesting/incorrect ... show more	Brute-Force SSH
✔ AdrianT	13 hours ago	SSH brute force	Brute-Force SSH
✔ ZeroAttackVector	14 hours ago	zrh: 3 unauthorised SSH/Telnet login attempts between 2022-07-04T03:50:20Z and 2022-07-04T03:57:29Z	Brute-Force SSH
✔ M127	14 hours ago	Jul 4 03:49:49 scw-tender-jepsen sshd[18272]: Failed p assword for root from [redacted] port 5892 ... show more	Brute-Force SSH

TRUXGO

¿QUÉ ES UN REPORTE DE ABUSE?

Es una solicitud en la cual se reporta una falta a las políticas de uso aceptable del servicio de internet, realizada por una dirección IP, domino web, servidor o servicio.

TRUXGO

¿POR QUÉ TENGO REPORTES DE ABUSE?

- Configuraciones erróneas.
- Uso inadecuado de los recursos.
- Reportes de la comunidad.
- Falsos positivos.

TRUXGO

CAUSAS FRECUENTES

- SPAM
- DDOS
- Phishing
- Port Scaning
- Virus / Malware
- Configuraciones erróneas
- Copyright

TRUXGO

PÉRDIDAS OCASIONADAS POR ESTAR EN UNA BLACKLIST

TRUXGO

Estar en una blacklist representa un problema serio para cualquier organización, ya que afecta tanto la comunicación como la imagen y las finanzas de la empresa.

TRUXGO

A continuación, se presentan las principales consecuencias:

Pérdidas económicas:

Los bloqueos pueden generar reducción en ventas, cancelaciones de servicios y costos adicionales para limpiar la reputación y recuperar la normalidad operativa.

TRUXGO

TRUXGO

Clientes molestos o insatisfechos:

Cuando los correos legítimos no llegan a su destino, los clientes pueden sentirse ignorados o mal atendidos, provocando quejas o incluso la pérdida de relaciones comerciales.

Daño a la reputación:

La marca pierde credibilidad ante clientes, socios y proveedores, afectando su confiabilidad y profesionalismo.

TRUXGO

Interrupción de la comunicación:

La empresa puede tener dificultades para enviar o recibir correos importantes, impactando en la atención al cliente, la gestión de proyectos o la coordinación interna.

TRUXGO

Pérdida de oportunidades:

Al no poder comunicarse correctamente, se pueden perder propuestas, contratos o nuevos clientes potenciales.

TRUXGO

ACCIONES PREVENTIVAS

TRUXGO

¿QUÉ SE DEBE DE HACER?

Dar importancia al área y brindar presupuesto acorde a las necesidades

Facilitar otros medios de contacto

Integrar al centro de respuesta ante incidentes en los casos.

TRUXGO

¿QUÉ SE DEBE DE HACER?

Establecer políticas preventivas en la entrega de los servicios.

Hacer monitoreo frecuente de los recursos.

Colaborar con el CSIRT-CERT.

TRUXGO

¿QUÉ SE DEBE DE HACER?

Especializar un departamento de ABUSE.

Identificar el servicio que se le da a los recursos otorgados al usuario final.

Coordinación directa ante eventos críticos.

TRUXGO

¿QUÉ SE DEBE DE HACER?

Identificar el uso que se le dará a los recursos.

Notificar las políticas de uso aceptable.

Coordinación directa ante eventos críticos.

TRUXGO

ACCIONES CORRECTIVAS

TRUXGO

¿QUÉ SE DEBE DE HACER?

Tener un programa de soluciones críticas sobre recursos afectados.

Facilitar los procesos y presupuestos ante el evento.

Coordinar acciones con las áreas involucradas.

TRUXGO

¿QUÉ SE DEBE DE HACER?

Identificar causa y motivo del reporte

Verificar si se incumplieron políticas de entrega

Enviar evidencias al CSIRT-CERT

Contactar a la entidad del reporte y determinar acciones

TRUXGO

¿QUÉ SE DEBE DE HACER?

Brindar protocolo de identificación.

Comunicar el reporte a la área responsable.

Brindar soluciones alternas al cliente.

Dar comunicado final (positivo-negativo).

TRUXGO

SOLUCIONES BASES

TRUXGO

LOS RECURSOS DEBEN ESTAR SUB ASIGNADOS

TRUXGO

LAS DIRECCIONES DEBEN CONTAR CON PRT

DNS Lookup (A Record)

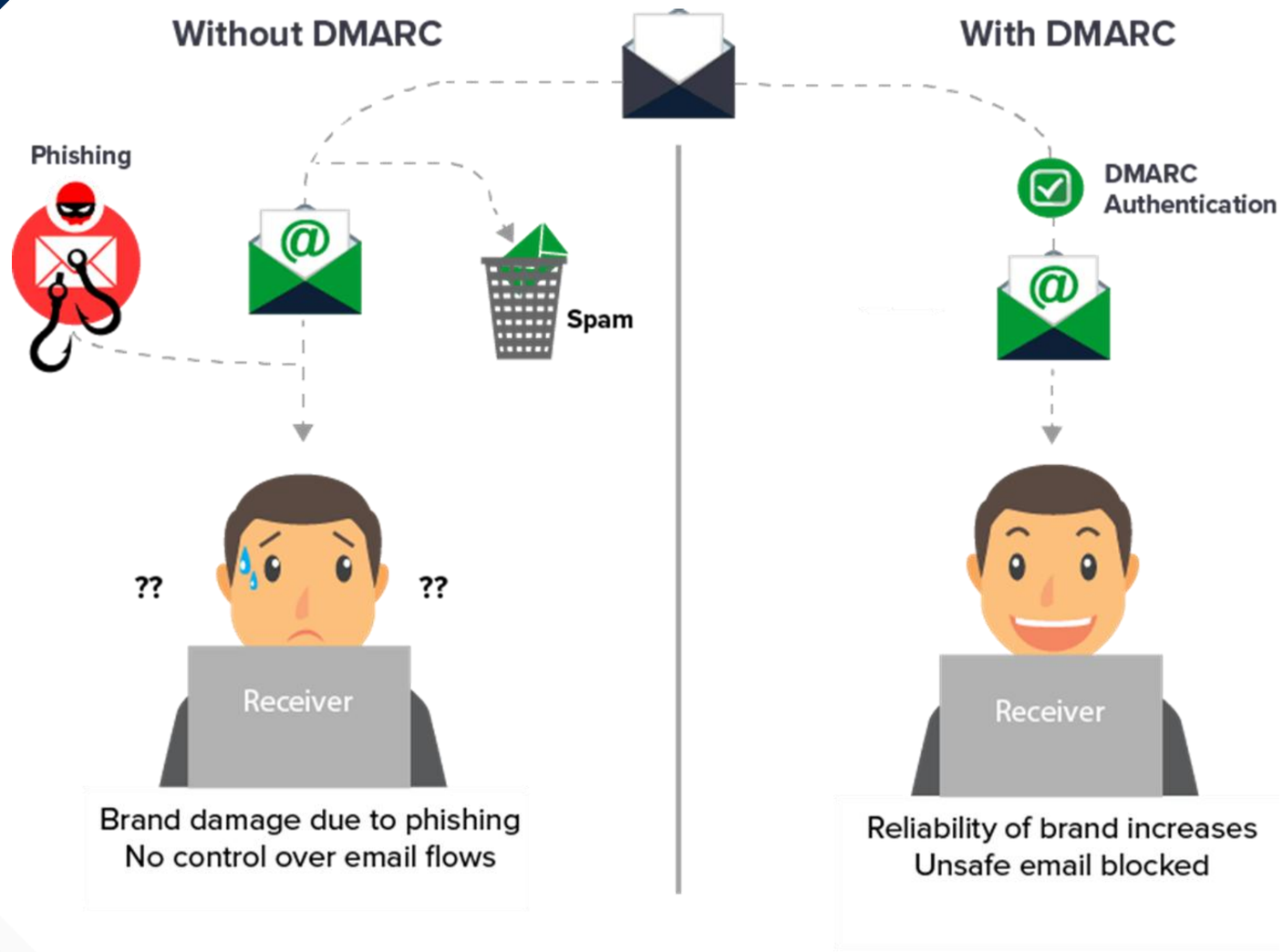
truxgo.com → 131.196.253.94

DNS Lookup (A Record)

truxgo.com → 131.196.253.94

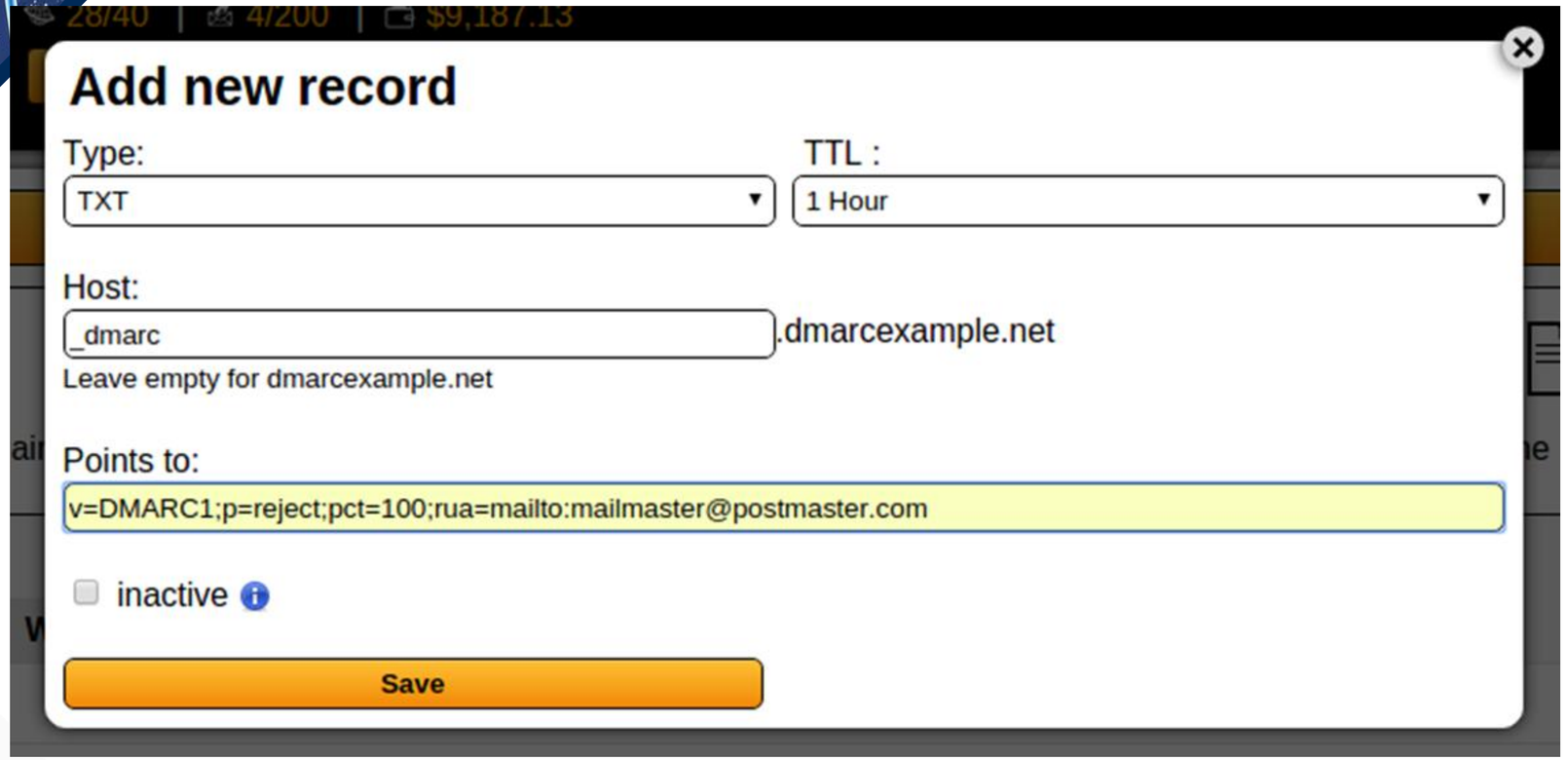
TRUXGO

DEBEN CONTAR CON DMARC



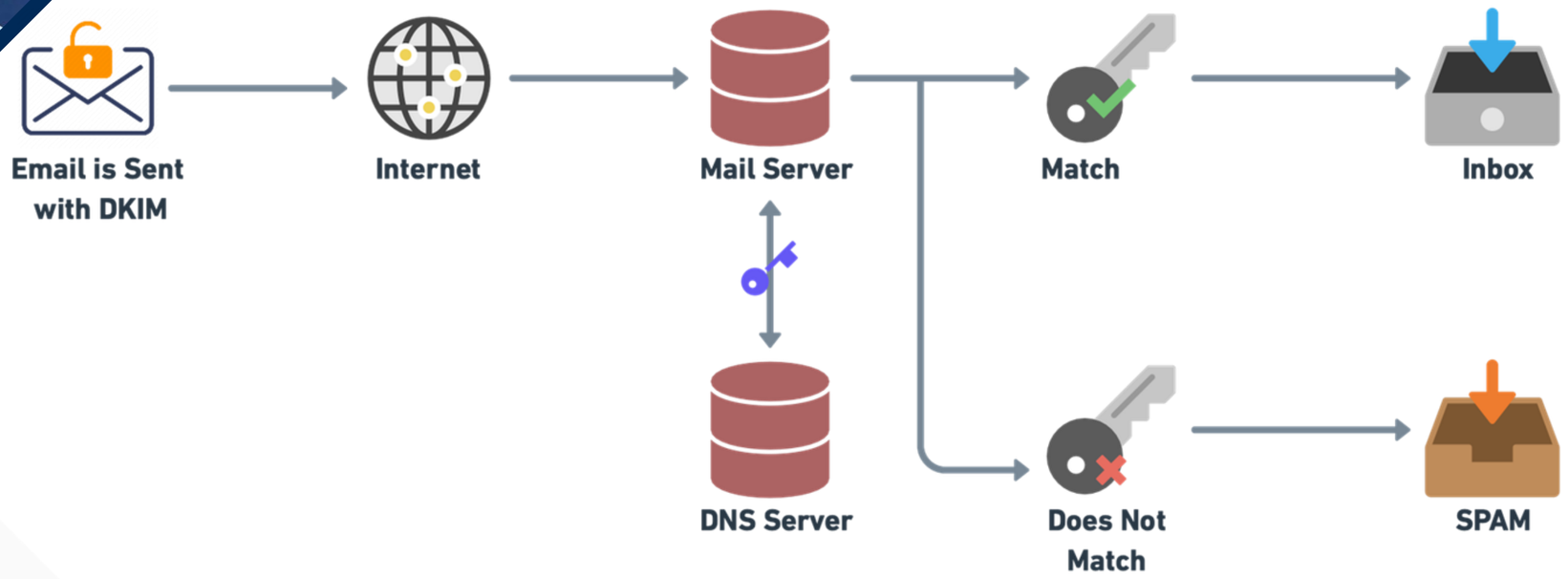
TRUXGO

DEBEN CONTAR CON DMARC



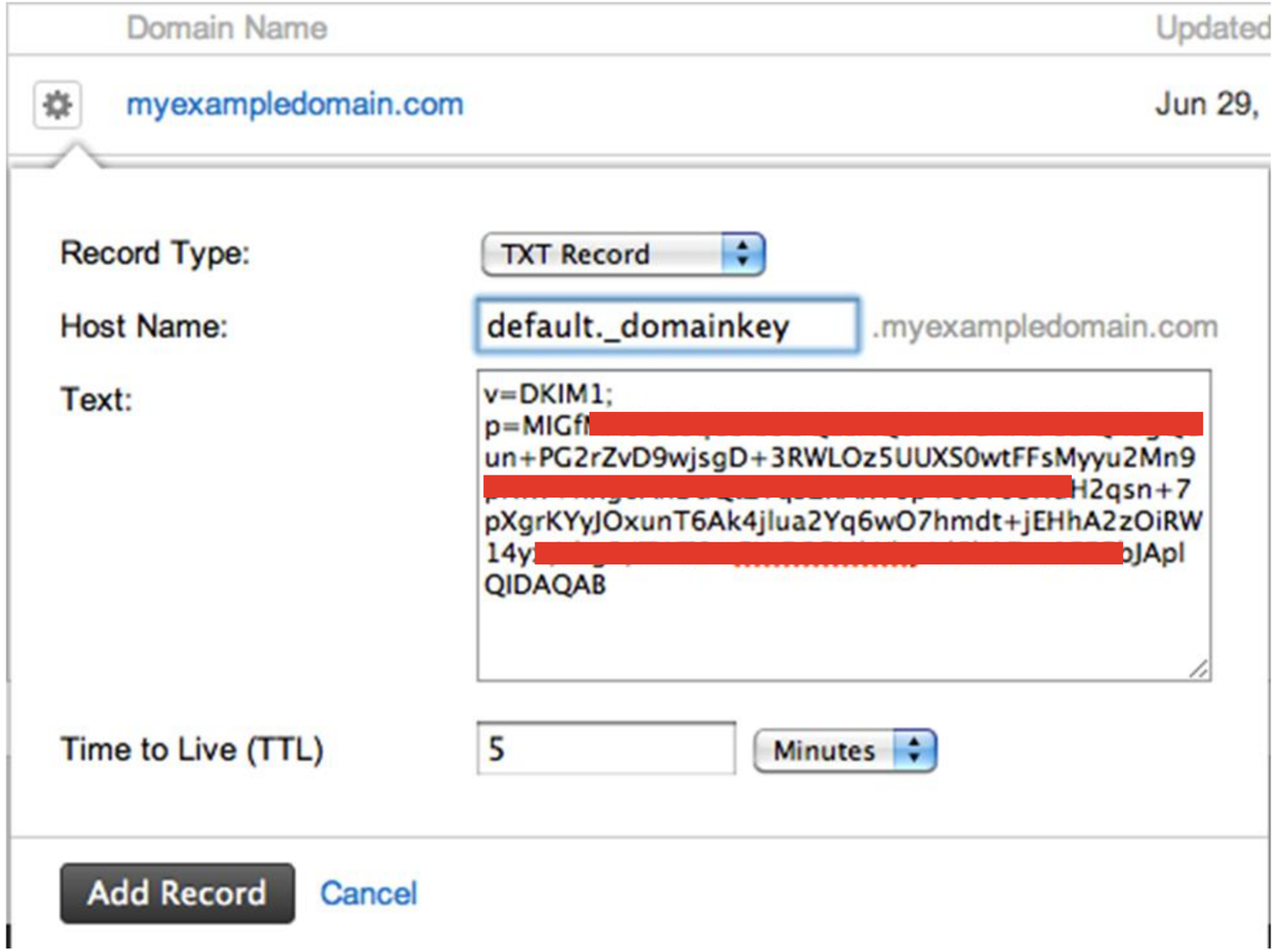
TRUXGO

DEBEN CONTAR CON DKIM



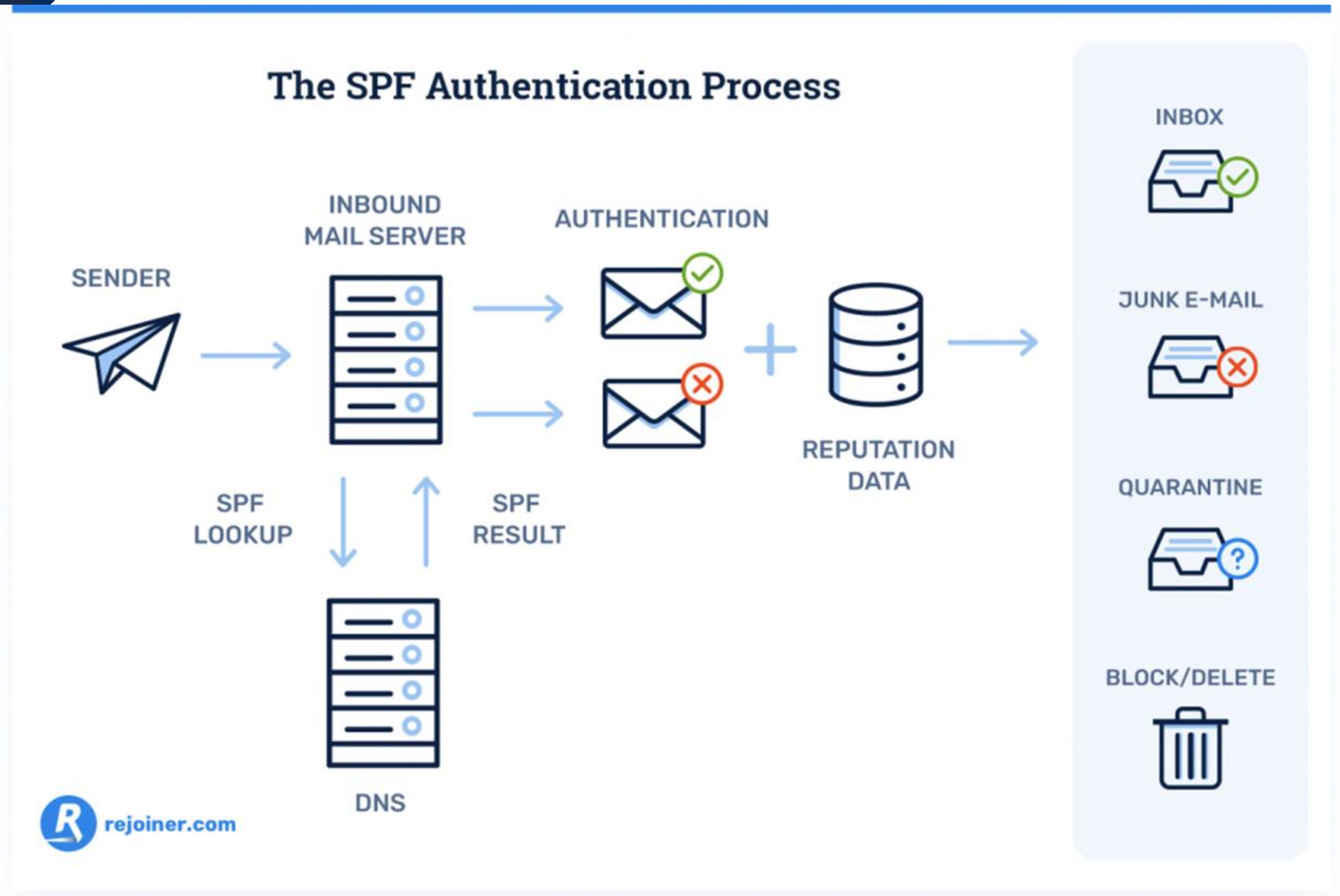
TRUXGO

DEBEN CONTAR CON DKIM



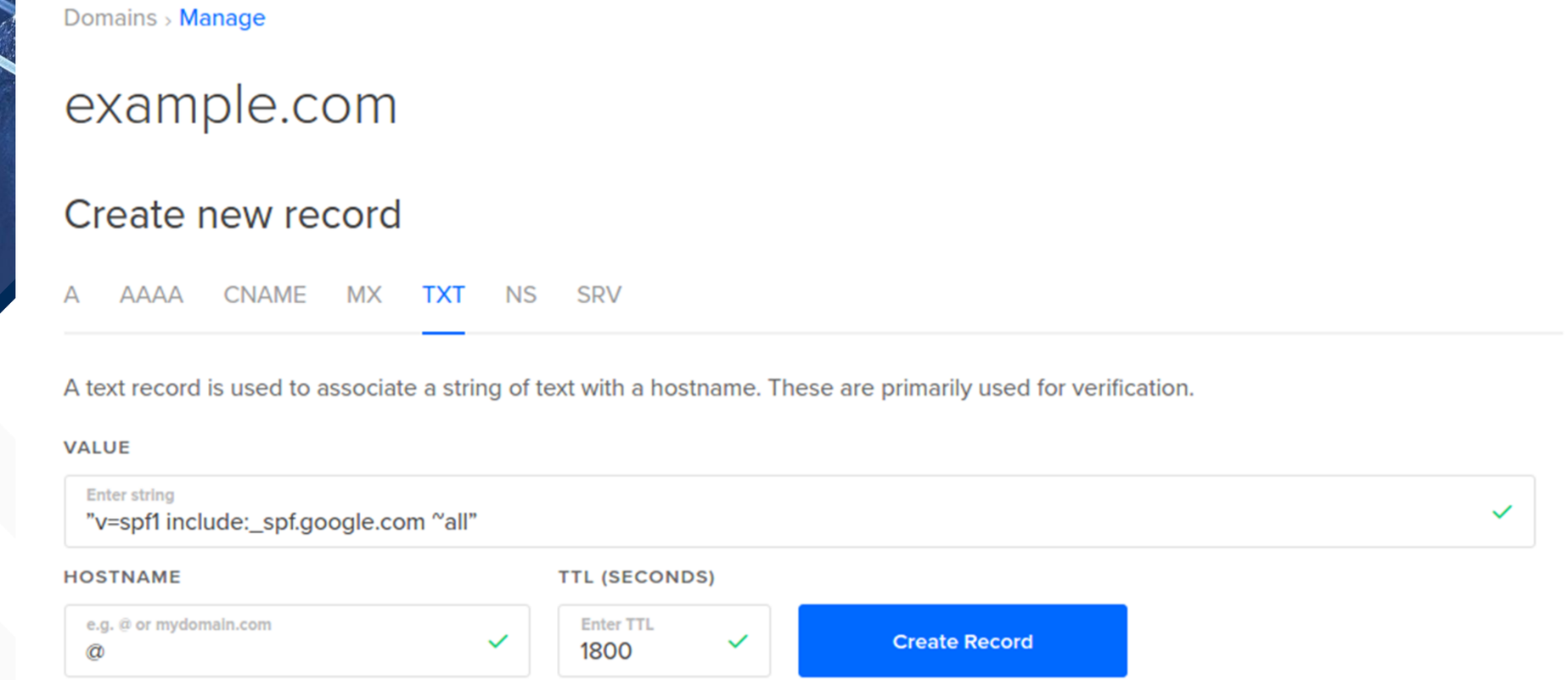
TRUXGO

DEBEN CONTAR CON SPF



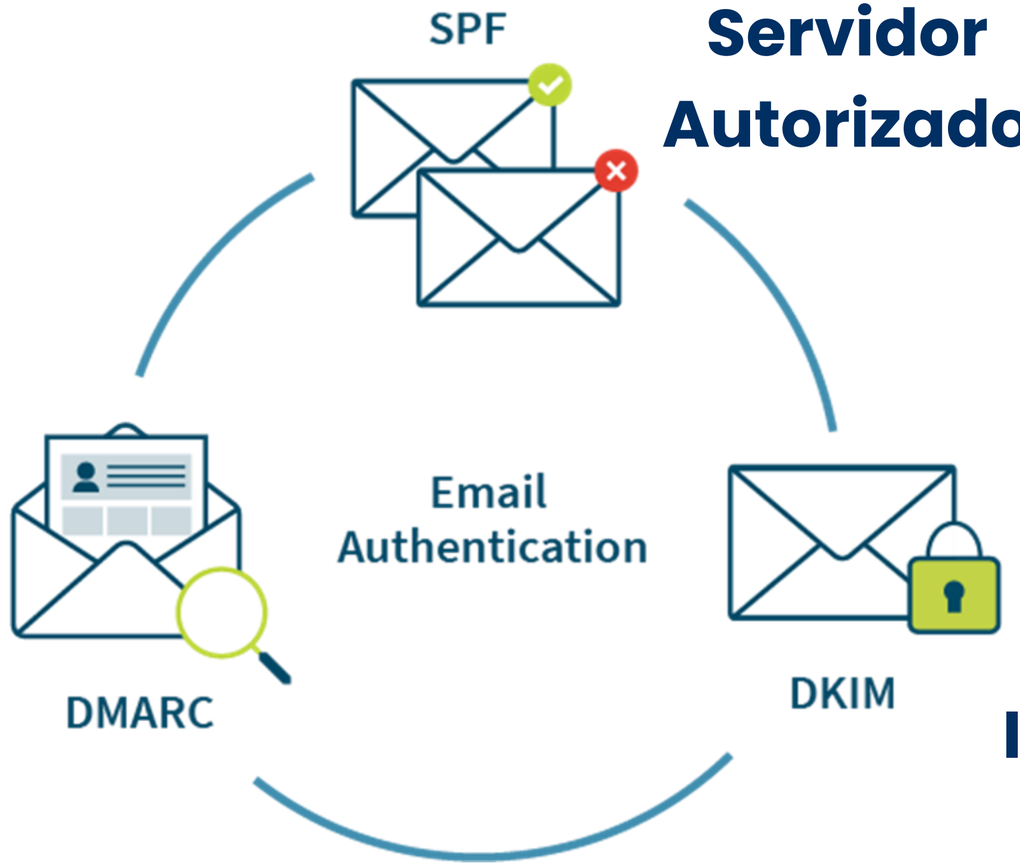
TRUXGO

DEBEN CONTAR CON SPF



TRUXGO

LOS 3 SON NECESARIOS



Servidor Autorizado

Contacto Responsable

Llaves de Identificación

TRUXGO

BLOQUEO DE PUERTOS

25

80

21

TRUXGO

TIPOS DE ORGANIZACIONES

TRUXGO

SPAMHAUS

Dificultad: ★★★

Categorías: SBL / XBL / PBL / DBL / ZEN / CSS
Tiempo: Definido por las categorías

Especialidad: SPAM / Phishing
Reporta: IPv4 / IPv6 / ASN / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: Definido por las categorías

Barracuda

Dificultad: ★★★★

Categorías: General
Tiempo: 2 semanas – 2 meses

Especialidad: SPAM / Virus
Reporta: IPv4 / IPv6 / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: Si

TRUXGO

spamcop.net

Dificultad: ★

Categorías: BL Spamcop
Tiempo: Definido por categoría

Especialidad: SPAM
Reporta: IPv4 / IPv6 / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: Si

AbuseIPDB

Dificultad: ★★★★★

Categorías: Spam / Hacking / Botnets / DDOS / Phishing
Tiempo: Definido por las categorías

Especialidad: Spam / Hacking / Botnets / DDOS / Phishing
Reporta: IPv4 / IPv6
Bloqueo: Puede bloquear desde una dirección IP
Avisos previos: No

TRUXGO

Dificultad: ★★★★★

Categorías: RatsDYNA / RatsnoPTR / RatsSPAM/ RatsnoAuth
Tiempo: Definido por las categorías

Especialidad: SPAM
Reporta: IPv4 / IPv6 / ASN / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: No

TRUXGO

.gov

Dificultad: ★★★★★

Categorías: Spam / Hacking / Botnets / DDOS / Phishing / Geo
Tiempo: Definido por categoría

Reporta: IPv4 / IPv6 / Dominios / DNS
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: No

Dificultad: ★★★★★

Categorías: VPN / Proxy / Geo / DDOS
Tiempo: Definido por las categorías

Especialidad: Spam / Hacking / Botnets / DDOS / Phishing
Reporta: IPv4 / IPv6
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: No

TRUXGO

Dificultad: ★★★★★

Categorías: Spam / Hacking / Botnets / DDOS / Phishing / Geo

Tiempo: Definido por categoría

Reporta: IPv4 / IPv6 / Dominios / DNS

Bloqueo: Puede bloquear todo el prefijo asignado

Avisos previos: No

Dificultad: ★★★★★

Categorías: Spam / Hacking / Botnets / DDOS / Phishing / Reputación

Tiempo: Definido por las categorías

Especialidad: Spam / Hacking / Botnets / DDOS / Phishing

Reporta: IPv4 / IPv6 / ASN / Dominios / DNS

Bloqueo: Puede bloquear todo el prefijo asignado

Avisos previos: No

TRUXGO

GRACIAS

Jorge Varela

TRUXGO

Ventas@corp.truxgo.com

+52 221 248 1630