Resumen ejecutivo

La **suplantación de identidad (spoofing) en el correo electrónico** sigue siendo una de las amenazas más prevalentes y efectivas en el panorama de la ciberseguridad actual, facilitando ataques de phishing, spam y compromisos de seguridad. Este documento técnico analiza en profundidad los fundamentos de este vector de ataque, basándose en una revisión exhaustiva de los mecanismos de funcionamiento del protocolo de correo electrónico, los puntos débiles intrínsecos en su diseño y las técnicas de explotación documentadas. Se examinan los mecanismos de verificacion diseñados para mitigar estos riesgos —SPF, DKIM y DMARC—, asi como sus limitaciones practicas.

1. Introducción y antecedentes

El **correo electrónico**, basado en el **Simple Mail Transfer Protocol (SMTP)**, fue diseñado en una era donde la confianza en la red era implícita. Su arquitectura original carecía de mecanismos robustos para **verificar la autenticidad del remitente**. Esta deficiencia fundamental ha sido explotada continuamente, permitiendo que actores maliciosos falsifiquen el campo FROM para hacer que un mensaje parezca originarse en una entidad legítima (como un banco, una compañía de servicios o un contacto conocido). Este tipo de ataque, denominado genéricamente **email spoofing**, es la puerta de entrada primaria para campañas de **phishing**, **Business Email Compromise (BEC)** y distribución de **malware**. Su efectividad radica no solo en la ingeniería social aplicada al contenido del mensaje, sino también en la capacidad de burlar las defensas técnicas mediante la explotación de configuraciones laxas o la comprensión insuficiente de los controles de autenticación existentes.

Email/SCAM/Spoofing/Phissing

La suplantación real de email, depende en gran medida de:

1.- Dominios sin verificaciones SPF, DMARK, DKIM configuradas en sus DNS autoritativos, de como se construye el correo, cabeceras X Mailer y si la IP origen esta ya en lista negra (Blacklist) de SPAM.

2.- De la posibilidad de modificar el valor del campo FRORM del email origen; El servidor de correo destino no siempre verifica la direccion email origen;

3.- Sin filtros de entrada!, configuración laxa sin comprobar verificaciones; de la política DMARK (permitir, cuarentena o denegar) en el servidor de entrada en destino, con verificaciones falsisifcadas o sin verificar listas negras IP en la recpeción del correo eletronico; . Se podria hacer spoffing email, enviando desde SMTP de tercerlos ó un SMTP postfix propio en localhost, montado sobre Kali

Linux, con scripts en bash shell, python. De las cabeceras X Mailer y si la IP origen esta en listas negras IPv4, - **en IPv6 no hay blacklist!**

4.- Engaño usando el campo “display-name” como simulación visual del email origen cuando en destino hay niveles maximos de comrprovacion de las verificaciones de entrada, la rigurosidad de las verificaciones es maxima: SPF, DKIM, DMARK, Auth TLS, puerto 25/TCP, X Caveceras, Blacklist IP,... y filtrado del email. p. ej.: gmail, hotmail, yahoo, protonmail,. o con simulacion visual de caracteres, formando palabras parecidos al suplandado.

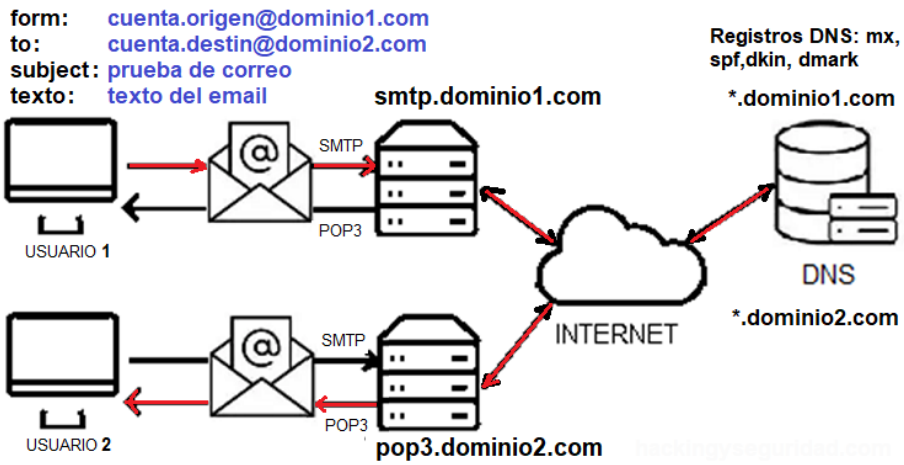
2. Fundamentos técnicos del envío de correo y puntos de falla

El proceso de entrega de un correo electrónico involucra múltiples componentes interconectados, cada uno de los cuales puede representar un punto potencial de explotación si no está correctamente configurado.

2.1. Proceso de envío

1. **Composición**: Un cliente (Outlook, Thunderbird, script Python/Bash..) define los campos FROM (que incluye un "display-name" y una dirección de email origen), TO, Subject y cuerpo. FORM: “display-name nombre a mostrar" < cuenta.origen@dominio1.com > **email origen** TO: cuenta.destino@dominio2.com, indicamos la **dirección de email del destinatario**, Subject: asunto del email y yexto: correo electronico ..
2. **Conexión SMTP**: El cliente conecta y se autentica con un servidor SMTP saliente.
3. **Resolución DNS**: El servidor SMTP consulta los registros **MX (Mail Exchanger)** del dominio destino para identificar su servidor IP/fqdn de correo entrante destino. Verificaciones DNS: El servidor SMTP realiza varias consultas, verificaciones para asegurar la entrega e impedir la suplanación/spam. Registro TXT, SPF (Sender Policy Framework): El servidor del destino verifica en el DNS autoritativo del dominio origen si la IP del servidor SMTP que está enviando el correo está autorizada para enviar correos en nombre de dominio1.com. Esto genera una verficiacion SPF, para evitar la suplantación de identidad (spoofing). Registro TXT, DKIM (DomainKeys Identified Mail): Es una "firma digital" del mensaje que también se verifica contra un registro DNS del dominio origen, garantiza la integridad. Registro TXT, DMARC (Domain-based Message Authentication, Reporting & Conformance): Política publicada en DNS que le dice al receptor qué hacer si fallan SPF o DKIM (ej: rechazar el correo).

4. **Entrega y almacena en la caperta de la cuenta de destino**: Se establece una conexión directa con el servidor POP3, IMAP de destino y se transfiere el mensaje usando el protocolo SMTP/ESMTP.
5. **Verificación en destino**: El servidor receptor ejecuta políticas de filtrado y verificación (listas negras IP, blacklist).
6. **Entrega**: Si se superan las verificaciones, el mensaje se almacena en el buzón del destinatario, accesible vía **POP3** o **IMAP**.



3.- Puertos y servicios

SMTP (Simple Mail Transfer Protocol) es un protocolo de comunicación estándar de Internet para dar salida, enviar correos electrónicos (email).

Puertos usuales TCP: 25, 587, 465, 110, 143, 995, 993

SMTP Simple Mail Trasport Protocol. el servicio en un servidor activo, normalmente usa el puerto TCP: 25, 587 y 465 con SSL/TLS, 2525, 25025

ESMTP (Extended Simple Mail Transfer Protocol), extension de SMTP con mas comandos de control

S/MIME (Secure/Multipurpose Internet Mail Extensions):

POP3 (Post Office Protocol)::110 y 995 con SSL/TLS

IMAP (Internet Message Access Protocol): 143, 993 con SSL/TLS

4.- Registros DNS de seguridad, protocolos y firmas; para evitar suplantacion SCAM/Spoofing/Phissing

DNS autoritativos; son los servidores maestros que contienen la información oficial y definitiva de un dominio.

Tipos principales de registros DNS:

A/AAAA : Asocian dominio → IPv4 (A) o IPv6 (AAAA)

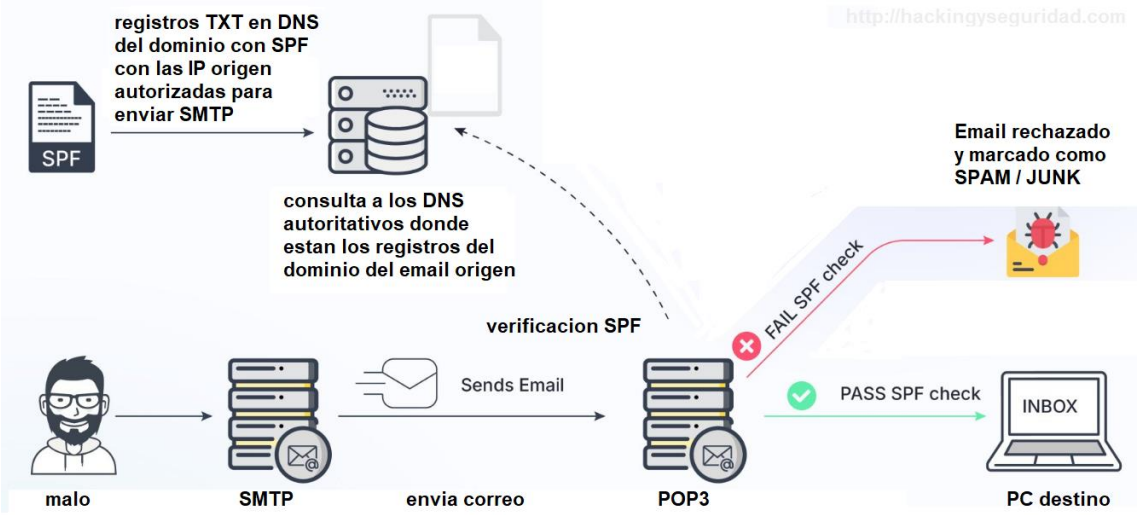
CNAME : Crea alias (ej: www apunta a dominio principal)

NS : Indica qué servidores DNS son autoritativos para el dominio

MX (Mail Exchanger): tipo de registro DNS, MX: Especifica servidores de correo electrónico. que determina el fqdm del servidor de correo electrónico para un dominio. MX "intercambio de correo" en un registro en la configuración DNS de un dominio , apunta a los nombre de los servidores de correo electrónico.

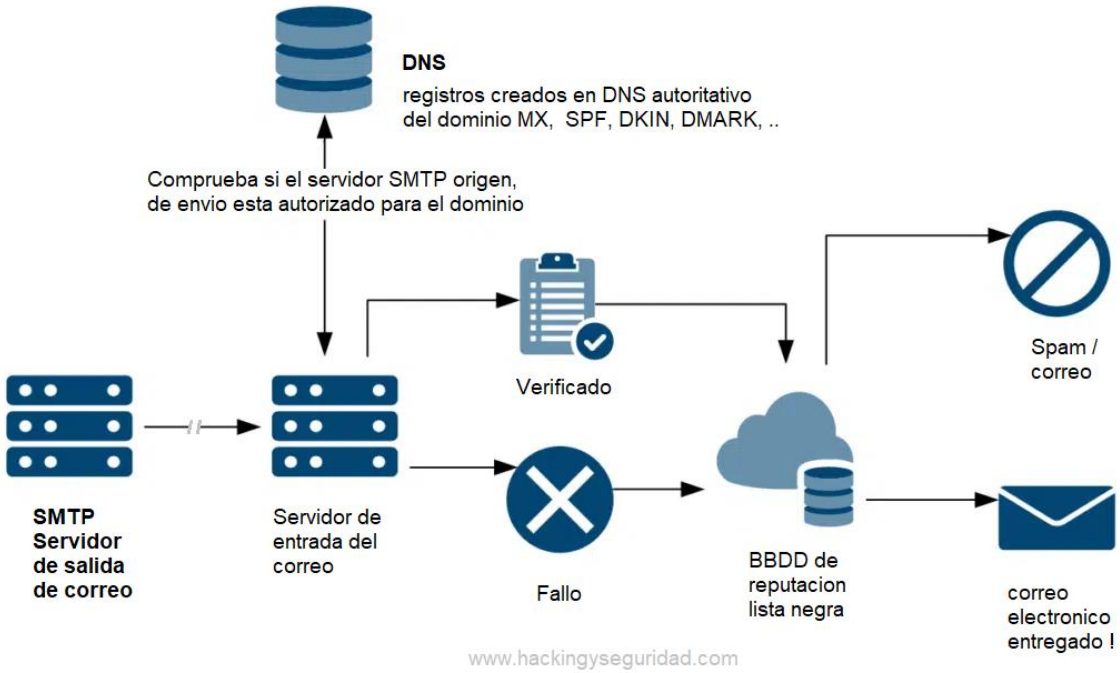
TXT : Almacena información textual (verificaciones, seguridad)

SPF, DKIM y DMARC sirven para autentificar a los remitentes de correo electrónico y cerificar que los correos electrónicos proceden del dominio del que dicen proceder. Estos tres métodos de autenticación son importantes para evitar el spam, los ataques de phishing y otros riesgos de seguridad

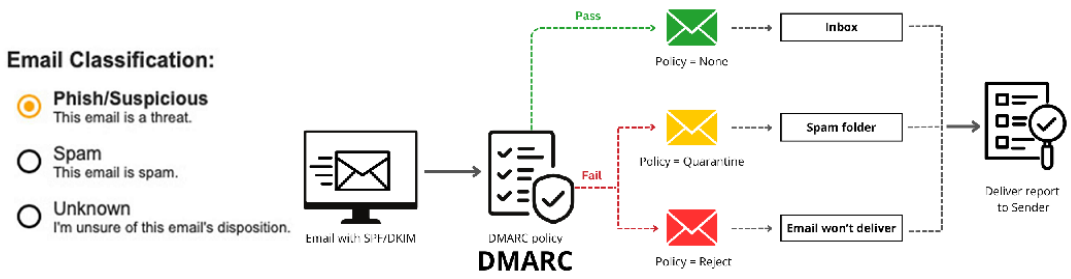


SPF, (Sender Policy Framework) es un tipo de resgistro en DNS autoritativo del dominio, donde se especifica los hostname o IP de los servidores de correo saliente, SMTP autorizados, para enviar con el nombre de ese dominio.

DKIN, (DomainKeys Identified Mail) protocolo de identidad, integridad que inserta firma cifrada en la cabecera del email, que certifica al destinatario que es veridico.



DMARK, (Domain-based Message Authentication, Reporting, and Conformance) es una política de correo electrónico que combina, tiene en cuenta SPF y DKIN, para confirmar la legitimidad del dominio en el origen FROM del email, la autenticación coincida con el dominio del «From:». **Uso:** Define políticas para manejar emails que fallan SPF/DKIM y reporta resultados.
DMARC tiene 3 niveles de seguridad: 1º.- (No hacer nada / monitorizar) 2º.- (Poner en Cuarentena) 3º.- (Rechazar)



Configuración:

- Registro **TXT** en el DNS autoritativo del dominio
- Nombre: _dmarc.tudominio.com
- Ejemplo: v=DMARC1; p=quarantine; rua=mailto:reportes@tudominio.com

Resumen de ubicación:

Registro	Tipo DNS	Donde se configura
SPF	TXT	Panel DNS del dominio
DKIM	TXT	Subdominio específico en DNS
DMARC	TXT	_dmarc subdominio en DNS

Importante: Los tres trabajan juntos para mejorar la deliverabilidad y prevenir spoofing/phishing.

**Limitaciones: **

Google/Gmail, Hotmail/Outlook p.ej: son mas estrictos: Requiere autenticación completa (SPF+DKIM+DMARC), para superar los filtros de entrada y que se entregue el correo.

IP residencial: Las IP de casa suelen estar bloqueadas para envío SMTP: https://check.spamhaus.org/ https://mxtoolbox.com/blacklists.aspx

El dominio usado debe tener DNS configurados . Los dominios nuevos tienen menos reputación

5.- Suplantar dirección de email, correo electronico . 10 tecnicas de SCAM/Spoofing/Phissing.

1º.- Manipulando el campo "FROM". del email origen, con script de envio.- algunos servidores SMTP (Simple Mail Transfer Protocol) no verifican el remitente FORM. https://github.com/hackingyseguridad/email/blob/main/enviopythonsmtp.py

2º.- Modificación de cabeceras X-Mailer del correo : cabeceras del email como: "From", "Reply-To" o "Return-Path",.. con scripts de envio ... https://github.com/hackingyseguridad/email/blob/main/suplantacongmailcabeceras.py

3º.- Uso de servidores SMTP Open Relay (sin autenticación), no seguros: pueden usarse estos servidores de correo mal configurados o comprometidos para enviar emails, de forma libre, modificando el FROM y/o cabeceras X-Mailer

4º.- Explotación de un servidor SMTP, por fuerza bruta o explotando otras vulnerabilidades CVE.

5º.- Compromiso de cuentas reales :Si un atacante obtiene acceso a una cuenta de correo legítima (por ejemplo, mediante phishing, fuerza bruta o credenciales robadas.

6º.- Uso de herramientas automatizadas : scripts (como PHPMailer o programas de envío masivo) que facilitan la falsificación de correos.

7º.- Uso de un dominio muy parecido ; (Typosquatting) Registro de dominios visualmente parecidos al legítimo, que visualmente sea disficil de notar que existe un caracter distinto.

8º.- Uso de un servidor SMTP, DNS, propio, ad hoc que simule las cuentas, dominio, falsifique registros y verificaciones: SPF, DKIM, DMARK. (DMARK modo, dejar
pasar). https://github.com/hackingyseguridad/email/blob/main/enviolocalhostdnark2.py

9º.- Uso de SMPT de otros proveedores paraa engañar, simular la descripcion del email origen en el Form, si este SMTP no imprime datos del email origen real.

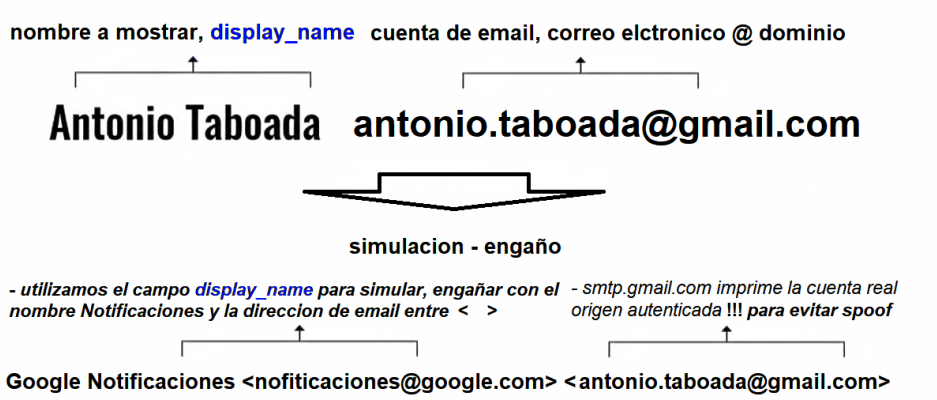
10º.- Uso de un servidor SMTP, que este en el SPF de otros dominios, comparte infraestructura e IPs permitidas (diseño de la arquitectura de red).

6.- CONCLUSION: El exito del envio de correo depende de:

1º.- en origen: eliminar restricciones en la configuracion SMTP y como se construye el correo/Email.

2º.- en destino: filtros y niveles de comrprovacion de las verificaciones en la entrada del email. p. ej.: gmail, hotmail, yahoo, protonmail,..: tienen nivele altos para evitar SPAM;

- En estos casos utilizando sus mismos SMTP para enviar email, podremos solo modificar en el FROM el "Display-name" nombre a mostrar y simular en el nombre de la cuenta para
  mostrar suplantada@suplantado.com ,porque estos SMTP suelen imprimir siempre la cuenta de email real autenticada utilizada!



- Otros muchos proveedores de correo sin niveles de comprobacion en los filtros de entrada, mas laxos para rececpcion, hacen facil el SPAM/Phissing email, desde SMTP propios o de terceros!

7.- ENVIO: Scripts de composición del correo eletronico y envio:

1º.- con servidor SMTP de terceros (smtp.gmail, otros,..)

2º.- con un servidor propio SMTP "localhost", DNS propio!

Configuraciones servidor SMTP Postfix

Postfx como servidor SMTP

main.cf

main.cf gmail relay

9.- Proveedores gratuitos de envio de email.

Yahoo : smtp.mail.yahoo.com:587

Hotmail : smtp.live.com:587

Gmail de Google : smtp.gmail.com:25

Gmail de Google : smtp-relay.gmail.com:25

Microsoft Office 365 : smtp.office365.com:587

19.- Tracear un email con "ver correo original" en Gmail

https://support.google.com/mail/answer/29436?hl=es

10.- Temporal email para pruebas

https://temp-mail.org/es/