

PlaSysX

5 PUNTOS

**QUE ANALIZO EN UN
EMAIL SOSPECHOSO**



Saul Ruiz Plaza

1. Cabeceras del Correo

Antes del remitente, reviso los campos como:

From: muestra quién dice enviar el correo, pero puede estar suplantado.

Return-Path: dirección usada para rebotes. Puede revelar el servidor/dominio real de envío.

Received: muestra los saltos entre servidores de correo. Ayuda a rastrear el origen.

Message-ID: identificador único del mensaje
Puede dar pistas sobre el sistema que lo generó.

2. SPF, DKIM y DMARC

Analizaría si el correo supera las validaciones de autenticación del dominio.

SPF: valida si el servidor está autorizado para enviar correos en nombre del dominio.

Puede indicar posible suplantación si aparece como **spf=fail**.

DKIM: comprueba la firma criptográfica del mensaje.

Ayuda a saber si el correo fue modificado o si realmente lo firmó el dominio.

DMARC: define qué hacer si SPF o DKIM fallan.

Aplicar políticas como none, quarantine o reject.

3. Información del Dominio

Analizaría:

Dominio real: comprueba si el enlace pertenece realmente a la organización legítima.

Typosquatting: detecta dominios parecidos al original con letras cambiadas o añadidas.

Antigüedad del dominio: un dominio creado recientemente puede ser más sospechoso.

Certificado TLS: revisa si la web usa HTTPS y si el certificado tiene sentido.

Reputación de IP/URL: consulta si la IP o el enlace aparecen asociados a actividad maliciosa.

Hosting o ASN sospechoso: identifica si la infraestructura pertenece a proveedores usados en campañas maliciosas.

4. URLs, redirecciones y adjuntos

Analizaría a dónde llevan realmente los enlaces y qué tipo de archivos adjuntos incluye el correo.

URL visible: el texto del enlace puede decir una cosa, pero apuntar a otra web.

URL real: destino verdadero al que lleva el enlace al hacer clic.

Adjuntos: archivos que pueden contener macros, scripts o malware.

Extensión real: un archivo puede parecer PDF, pero acabar siendo .exe, .html o .docm.

Tipo MIME: ayuda a comprobar si el archivo realmente es lo que aparenta.

Hash del archivo: identificador único para buscar reputación o coincidencias en análisis.

5. Técnicas de Ingeniería social

Analizaría qué técnica psicológica usa el correo para intentar que la persona actúe sin pensarlo demasiado.

Urgencia: fuerza una acción rápida con mensajes como “último aviso” o “24 horas”.

Miedo: amenaza con bloqueos, sanciones o pérdida de acceso.

Autoridad: simula venir de un jefe, proveedor, banco o servicio conocido.

Confianza: usa logos, lenguaje corporativo o información real para parecer legítimo.

Curiosidad: intenta que abras un enlace o archivo porque parece importante.

Q. ¿Es Phishing?



mailbox.local / message



Acción requerida: actualización de acceso



Soporte NexaCloud
soporte@nexacloud-careers[.]com

Hoy, 09:42

From: Soporte NexaCloud <soporte@nexacloud-careers[.]com>
Return-Path: <bounce@secure-mail-login[.]com>
Reply-To: validacion@nexacloud-soporte[.]com
Received: from mail.secure-mail-login[.]com by mx.empresa.local

Hola, Saúl:

Hemos detectado una revisión pendiente en tu cuenta corporativa. Para evitar la suspensión temporal, confirma tus datos antes de 24 horas.

Este proceso forma parte de la actualización de seguridad del servicio.

Revisar cuenta

Destino del enlace:

[https://nexacloud-validacion\[.\]com/login](https://nexacloud-validacion[.]com/login)

DEJALO EN LOS COMENTARIOS



Saúl Ruiz Plaza

PlaSysX