Herramientas
para prevenir ataques de ingeniería social

mexus®

Managed secure IT | no matter what

Herramientas
para prevenir ataques de ingeniería social

Introducción

Los ciberdelincuentes cuentan con una gran variedad de técnicas dentro de su arsenal para llevar a cabo sus ataques de Ingeniería Social.
Por eso, en Mexis hemos desarrollado una serie de herramientas que permiten mejorar nuestra defensa.
Si actúa de manera proactiva, los ciberdelincuentes se las verán muy difícil para perpetrar en su organización.

En **Mexis** recomendamos afrontar la Seguridad de la Información mediante capas de protección, siendo la concienciación un factor fundamental para disminuir el riesgo de que sus usuarios se conviertan en víctimas de un ataque de Ingeniería Social.

Fraude del CEO

Un ciberdelincuente puede enviar correos a los usuarios de su organización suplantando la identidad de una persona de jerarquía, explotando su posición de influencia para realizar pedidos fraudulentos.
Si el servidor de correos corporativo no está configurado correctamente, un ciberdelincuente puede enviar los correos en nombre de una persona de alto mando desde el mismo servidor de la organización, evadiendo controles de seguridad como filtros de SPAM o registros SPF, DKIM y DMARC.

¡Descubra si su servidor de correos es vulnerable y cierre esta puerta a los ciberdelincuentes!

¿Está preparado su personal para identificar este tipo de ataque?

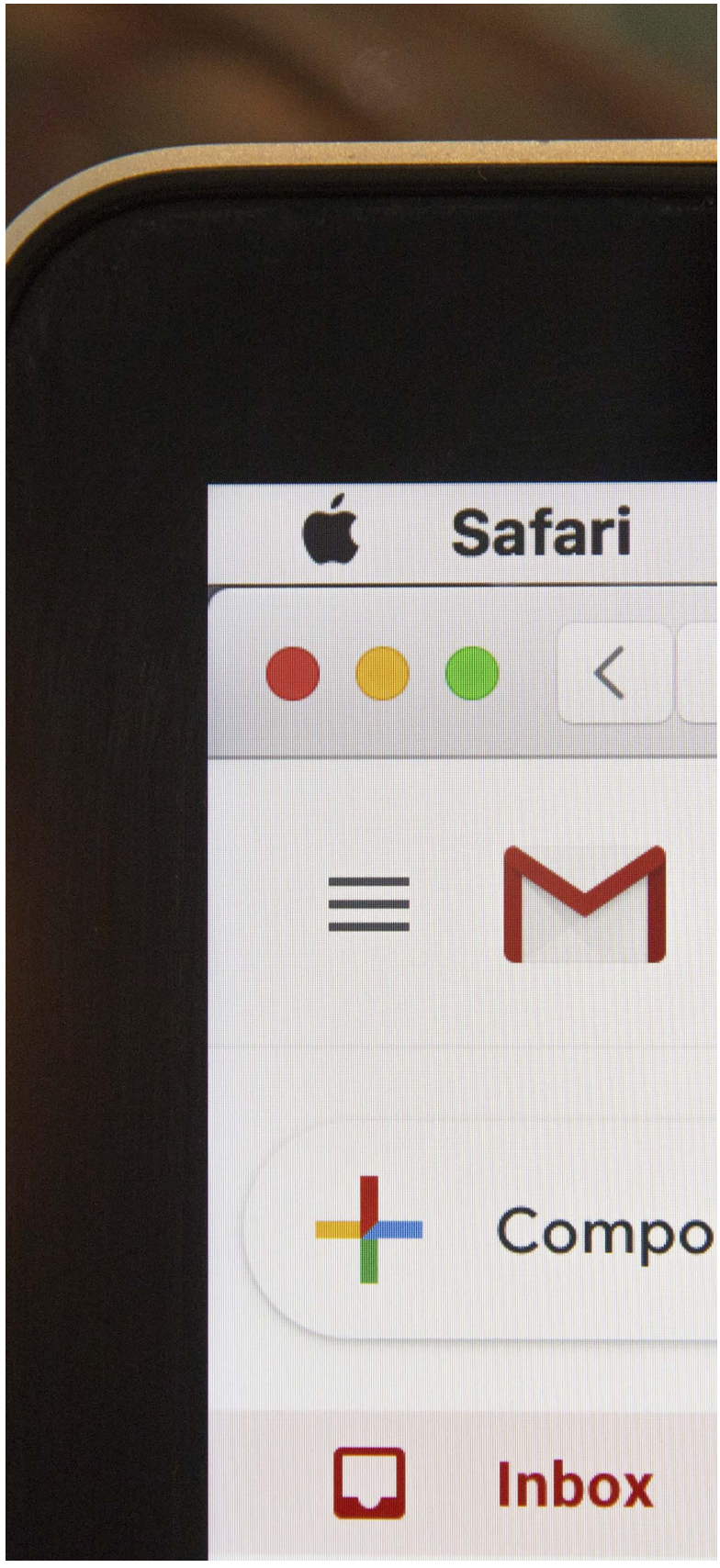
Spoof Check

Si el dominio de su organización no se encuentra correctamente protegido, un ciberdelincuente puede utilizarlo para enviar correos desde cualquier servidor de correos. Para proteger su dominio de manera correcta, debe implementar los siguientes protocolos:

- SPF: Identifica los servidores SMTP autorizados a enviar correos en un dominio.
- DKIM: Añade una firma digital a los correos legítimos mediante el uso de criptografía.
- DMARC: Aplica políticas de cuarentena y rechazo a correos que no cumplen con los protocolos SPF y DKIM.

¡Descubra si su dominio se encuentra protegido e impida su uso por parte de los ciberdelincuentes!

Conozca más nuestra herramienta.



mexus
Managed secure IT | no matter what

DNS Twist

Proteger su dominio y servidor de correo corporativo es indispensable para combatir la suplantación de identidad.
De todas maneras, esto no detendrá a un ciberdelincuente. Frente a esta protección, lo más común es que opte por utilizar un dominio similar al de su organización.
Para mitigar a este riesgo debe consultar de manera periódica los dominios similares que se encuentren registrados y controlar que pertenezcan a organizaciones legítimas.

¡Descubra los dominios similares al de su organización y controle su uso!
Conozca más sobre los fundamentos detrás de nuestras herramientas

Email Harvester

Un gran porcentaje de los ataques de suplantación de identidad se llevan a cabo mediante correo electrónico.
Un ciberdelincuente puede conocer las direcciones de email de los usuarios de su organización y enviarles correos de Phishing.

La manera más sencilla de obtener las direcciones es simplemente buscando aquellas que se encuentren expuestas en Internet.
¡Descubra el grado de exposición de las cuentas de correo electrónico de su organización y conciencie a los usuarios que las utilizan!
Conozca más sobre nuestras soluciones.

¡Contáctenos!