HACK BLOCK

Enero 2026 | Vol. 1

Estudio de Suplantación Empresarial en España

Radiografía del riesgo digital en España: Por qué la mayoría de las empresas permiten, sin saberlo, que ciberdelincuentes operen en su nombre.

El problema

El correo electrónico sigue siendo el principal canal de comunicación empresarial y, paradójicamente, el vector de ataque más explotado por el cibercrimen.

Mientras las inversiones en ciberseguridad se centran a menudo en cortafuegos o seguridad de servidores, una puerta fundamental permanece abierta en la mayoría de las organizaciones españolas: la identidad de su propio dominio.

En HackBlock hemos realizado un estudio masivo y análisis pasivo sobre una muestra de **10.167** dominios corporativos activos en España, abarcando desde microempresas hasta grandes corporaciones.

El objetivo ha sido determinar si la infraestructura digital española está preparada para detener el Email Spoofing (suplantación de identidad).

Los resultados de este estudio son una fotografía técnica de la realidad actual.
Y la conclusión es preocupante.

100 MILLONES DE CIBERATAQUES POR CORREO ELECTRÓNICO EN 2 AÑOS

SEGÚN TREND MICRO

Metodología del Estudio

Para garantizar la objetividad de los datos, el estudio se ha realizado mediante análisis OSINT (Open Source Intelligence) y revisión de registros DNS públicos. No se han realizado intrusiones ni escaneos activos agresivos.

El análisis se ha centrado en la presencia y correcta configuración de los tres pilares de la autenticación de correo:

- **SPF (Sender Policy Framework):** Quién tiene permiso para enviar correos.

- **DKIM (DomainKeys Identified Mail):** Firma criptográfica del mensaje.

- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Qué debe hacer el receptor si el correo falla las pruebas anteriores.

17.3% DE AUMENTO EN EL NÚMERO DE CORREOS DE PHISHING EN LOS ÚLTIMOS 6 MESES

SEGÚN KNOWBE4

RESULTADOS

De los 10.167 dominios analizados, hemos categorizado el nivel de riesgo en función de la estrictez de sus políticas de seguridad:

61,36% (6.238 Empresas)

1. ALTO RIESGO | Es posible suplantar
Más de 6 de cada 10 empresas analizadas carecen de una política DMARC efectiva o no tienen registros SPF configurados.

Estos negocios no tienen configurados registros DMARC o políticas estrictas.

Consecuencia: Un ciberdelincuente puede enviar correos usando su dominio exacto (@suempresa.com) sin que los filtros antispam lo detecten. Es el escenario ideal para el fraude del CEO o BEC.

15,77% (1.603 Empresas)

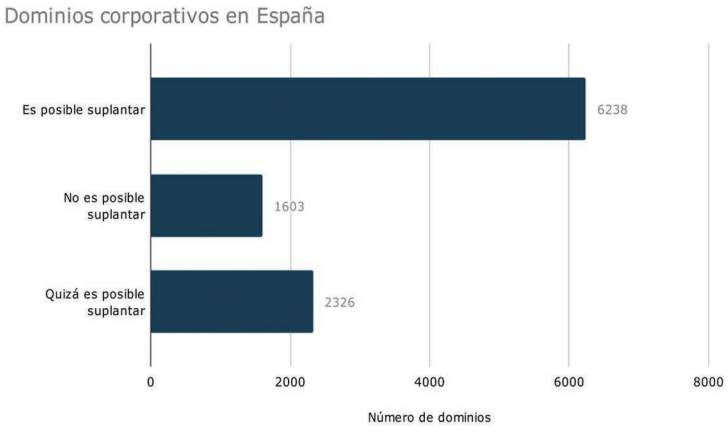
2. RIESGO MEDIO-ALTO | Quizá es posible suplantar
Tienen configuraciones parciales o permisivas (como p=none o errores de sintaxis).

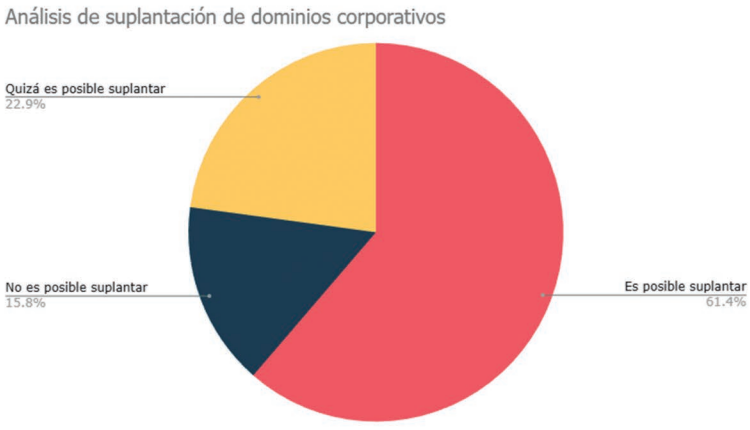
Aunque hay un intento de protección, no es suficiente para detener un ataque dirigido sofisticado. En muchas ocasiones esto significa que hay puerta abierta y depende del servicio de correo del receptor para recibir o no el correo como legítimo.

22,88% (2.326 empresas).

3. PROTEGIDOS | No es posible suplantar
Solo 2 de cada 10 empresas han "blindado" su identidad digital.

Sus dominios rechazan activamente cualquier correo que no salga de sus servidores autorizados.





El dato clave es que si sumamos el riesgo alto y medio, el 77% de las empresas analizadas son vulnerables a que su marca sea utilizada para estafar a clientes, proveedores o a sus propios empleados.

¿Por qué es alarmante este 77% de vulnerabilidad?

- El auge del "Fraude del CEO": La falta de protección DMARC es el facilitador técnico número uno para las estafas donde se solicitan transferencias urgentes a departamentos financieros.

- Daño Reputacional Silencioso: Muchas empresas no saben que están siendo suplantadas hasta que sus correos legítimos empiezan a caer en SPAM porque su dominio ha perdido reputación debido al abuso de terceros.

- Cumplimiento Normativo: Con la entrada de normativas más estrictas (como la directiva NIS2), la falta de higiene básica en los protocolos de comunicación empieza a ser un riesgo de compliance.

Conclusiones

La transformación digital en España ha avanzado en la nube y en la gestión de datos, pero ha descuidado los cimientos de la comunicación. Que en 2026 solo el 22% de las empresas tengan control total sobre quién usa su nombre en internet denota una falta de concienciación técnica grave.

Desde HackBlock, publicamos estos datos no para señalar culpables, sino para evidenciar una realidad: la tecnología de protección existe y es accesible, pero no se está implementando.

Es importante matizar que, incluso dentro del 22% de empresas "blindadas técnicamente", el riesgo cero no existe. Cuando el spoofing directo no es posible, los atacantes pivotan hacia el typosquatting (dominios similares) o la ingeniería social pura.

Por tanto, cerrar la brecha técnica del DMARC es solo el primer paso urgente. El siguiente, e inevitable, es fortalecer al usuario final ante lo que la tecnología no puede filtrar.

Sobre este estudio y fuentes

Este informe ha sido elaborado por HackBlock.

Hemos publicado el listado de empresas y su análisis en github por transparencia.

Los datos crudos y dominios han sido anonimizados para proteger la integridad de las empresas vulnerables detectadas.

Se puede acceder al listado a través de:
https://github.com/HackBlock/Estudio-de-suplantacion-empresarial-Spain-2026

¿Tu empresa es suplantable?

Desde HackBlock hemos desarrollado una herramienta web que permite descubrir en 30 segundos si un dominio es vulnerable y por lo tanto, puede ser suplantado.

Sin coste, publicamos la herramienta con objetivo de cambiar las estadísticas y crear concienciación empresarial.

Puedes acceder a la herramienta por el siguiente enlace:

https://hack-block.com/analisis

Hack-block.com

contacto@hack-block.com

Avenida El Altillo, P.I. Proxinave nave 6, 11405 Jerez de la Frontera, Cádiz.