Cómo los ciberdelincuentes están atacando a las PYMEs en Europa y África en 2025

Vectores de ataque clave que las PYMEs deben comprender para mantenerse protegidas

kaspersky

kaspersky.es

Introducción

Los ciberatacantes suelen ver a las pequeñas y medianas empresas (PYMEs) como objetivos más fáciles, asumiendo que sus medidas de seguridad son menos sólidas que las de las grandes empresas. De hecho, los ataques a través de proveedores, también conocidos como ataques de relación de confianza, siguen siendo uno de los tres principales métodos utilizados para vulnerar redes corporativas. Dado que las PYMEs generalmente están menos protegidas que las grandes empresas, esto las hace especialmente atractivas tanto para ciberdelincuentes oportunistas como para actores de amenazas sofisticados.

Al mismo tiempo, los ataques relacionados con IA se están volviendo cada vez más comunes, facilitando la preparación y adaptación rápida de campañas de phishing y malware, aumentando así su escala. Mientras tanto, las regulaciones de ciberseguridad se están endureciendo, lo que añade más presión de cumplimiento a las PYMEs.

Mejorar la seguridad nunca ha sido tan crítico. Kaspersky destaca los vectores de ataque clave que toda PYME debe conocer para mantenerse protegida.

.Las PYMEs en Europa y África son atacadas con malware que se hace pasar por aplicaciones empresariales

Cómo el malware y las aplicaciones otencialmente no deseadas (PUA) se disfrazan de servicios legítimos

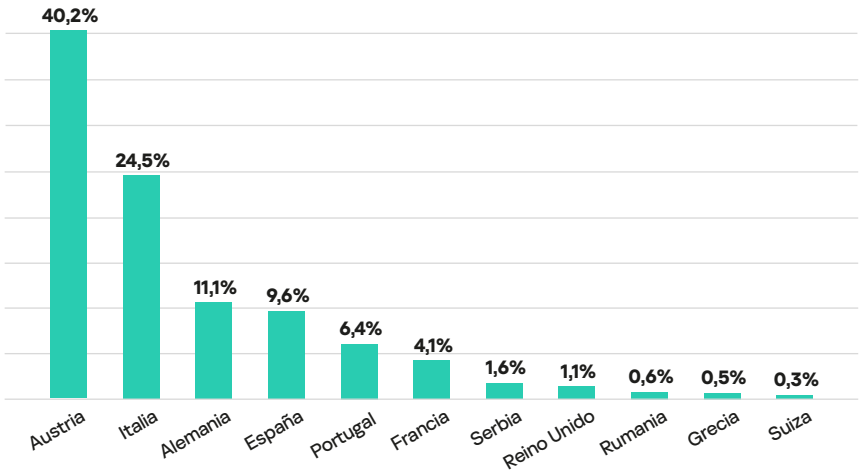
Los analistas de Kaspersky han utilizado datos de Kaspersky Security Network (KSN) para explorar con qué frecuencia archivos y programas maliciosos o no deseados se disfrazan como aplicaciones legítimas comúnmente usadas por PYMEs en Europa (Alemania, Austria, España, Francia, Grecia, Italia, Portugal, Reino Unido, Rumanía, Serbia y Suiza) y en algunos países seleccionados del norte, oeste y centro de África (Argelia, Camerún, Costa de Marfil, Marruecos, Senegal y Túnez). KSN es un sistema de procesamiento de datos anonimizados relacionados con ciberamenazas, compartidos voluntariamente por usuarios de Kaspersky. Para esta investigación, solo se analizaron los datos recibidos de usuarios de soluciones de Kaspersky para PYMEs. La investigación se centró en las siguientes aplicaciones:

- ChatGPT
- Cisco AnyConnect
- DeepSeek
- Google Drive
- Google Meet
- Microsoft Excel
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Teams
- Microsoft Word
- Perplexity
- Salesforce
- Zoom

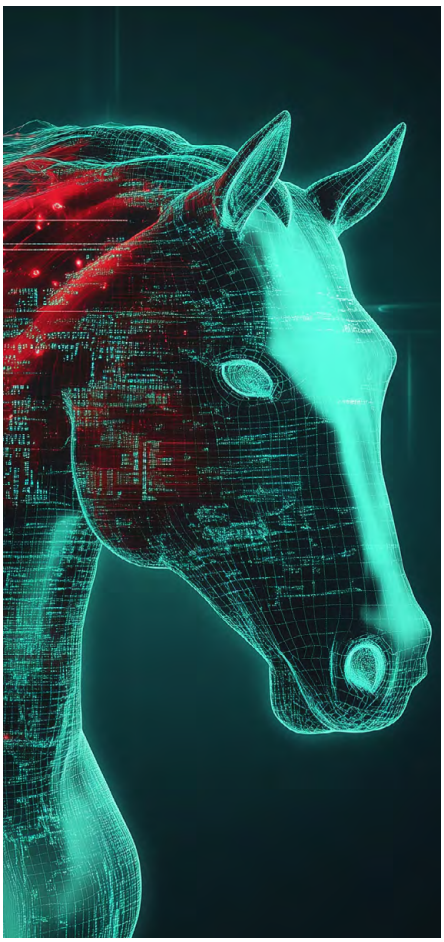
Panorama de amenazas para PYMEs en Europa

En 2025, Austria concentró la mayor proporción de ataques dirigidos a pequeñas y medianas empresas, acumulando el 40,2% de todos los casos detectados. Le sigue Italia con un 24,5% y Alemania con 11,1%. España y Portugal alcanzaron porcentajes del 9,6% y 6,4%, respectivamente. Francia registró un 4,1% de los casos, y Serbia y el Reino Unido cada uno alrededor del 1%. Otros países, incluyendo Rumanía, Grecia y Suiza, sumaron cada uno menos del 1% del total, lo que indica una actividad de ataque relativamente baja.

Distribución de ataques de malware y aplicaciones potencialmente no deseadas (PUA) que imitan aplicaciones legítimas en PYMEs en Europa[1]

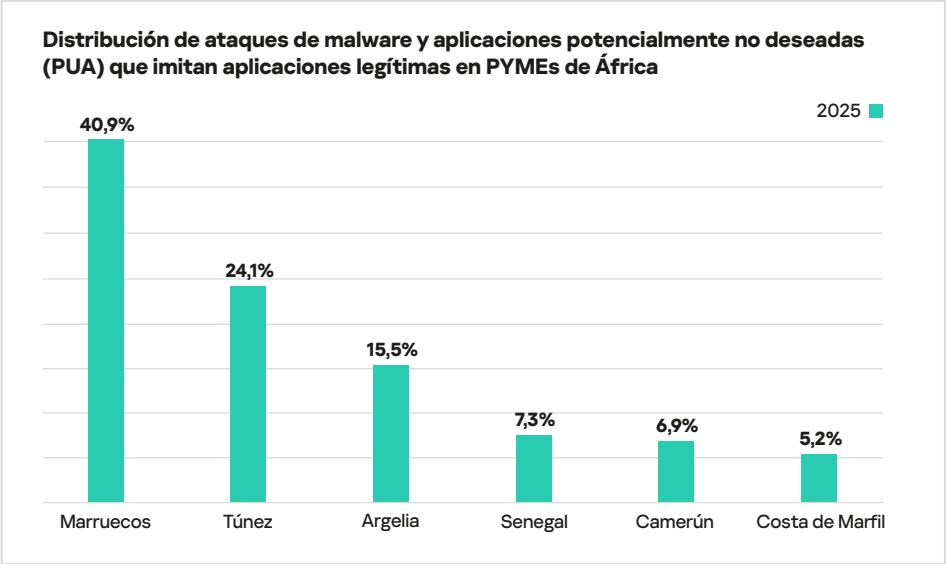


[1]El número de ataques en este informe indica cuántas veces los productos para PYMEs de Kaspersky detectaron malware o aplicaciones potencialmente no deseadas (PUAs) que imitaban marcas legítimas dentro de la muestra analizada.



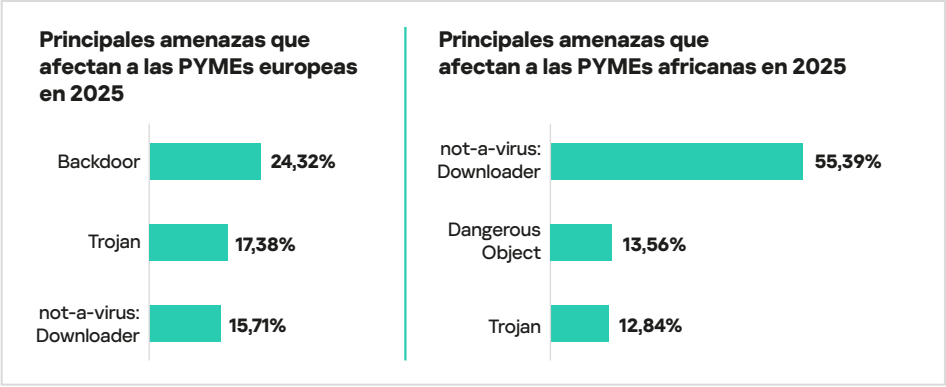
Panorama de amenazas para PYMEs en el Norte, Oeste y Centro de África

En 2025, Marruecos representó la mayor proporción de ataques entre los países africanos analizados, con un 40,9% de todos los casos detectados. Le siguen Túnez con un 24,1% y Argelia con un 15,5%. Senegal y Costa de Marfil registraron porcentajes más modestos, con un 7,3% y un 5,2% respectivamente. Camerún obtuvo un registro relativamente pequeño con un 6,9%.



Principales amenazas que afectan a las PYMEs

Las principales amenazas que afectan a las PYMEs en Europa incluyen backdoors (24,32%), troyanos (17,38%) y Downloaders (15,71%). Mientras que en África, downloaders fue el principal tipo de amenaza (55,39%), seguido de objetos peligrosos (13,56%) y troyanos (12,84%).



Los backdoors proporcionan a los ciberdelincuentes administración remota del equipo de la víctima. A diferencia de las herramientas legítimas de administración remota, los backdoors se instalan, se ejecutan y funcionan de manera invisible, sin el consentimiento ni el conocimiento del usuario. Una vez instalados, los backdoors pueden recibir instrucciones para enviar, recibir, ejecutar y eliminar archivos, recopilar datos confidenciales del ordenador, registrar la actividad y más.

En Europa, los backdoors representan **24.32%** de las amenazas a PYMEs; mientras que en África, los Downloaders dominan con un **55.39%**.

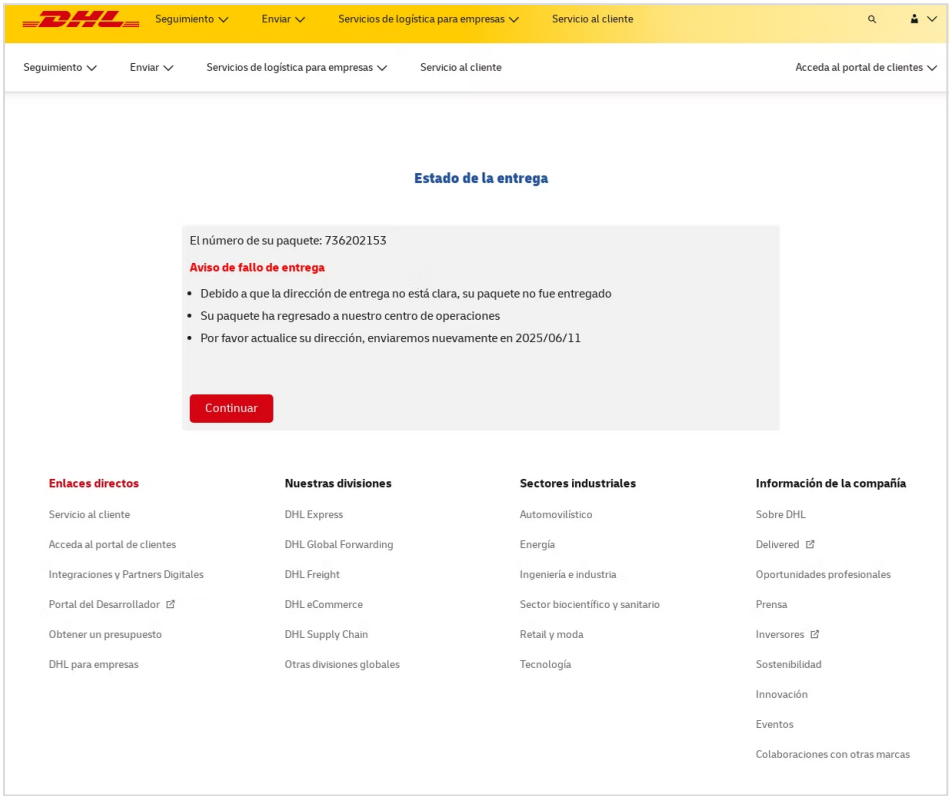
Por otro lado, los downloaders son aplicaciones potencialmente no deseadas diseñadas para instalar contenido adicional desde internet, a menudo sin informar de forma clara al usuario sobre lo que se está descargando. Aunque no son inherentemente maliciosas, estas herramientas son explotadas frecuentemente por atacantes para instalar cargas dañinas a los dispositivos de las víctimas. Los troyanos son programas maliciosos que realizan acciones no autorizadas, como eliminar, bloquear, modificar o copiar datos, o interrumpir el funcionamiento normal de computadoras y redes. Los troyanos se encuentran entre las formas de malware más frecuentes, y los ciberdelincuentes continúan utilizándolos en una amplia variedad de campañas maliciosas.

En cuanto a los objetos peligrosos, son objetos maliciosos que, por el momento, no cuentan con una clasificación precisa. Pueden incluir diversos tipos de malware, como troyanos o adware, así como otros archivos potencialmente no deseados o maliciosos detectados por las soluciones de Kaspersky.

Cómo los scammers y phishers engañan a las víctimas

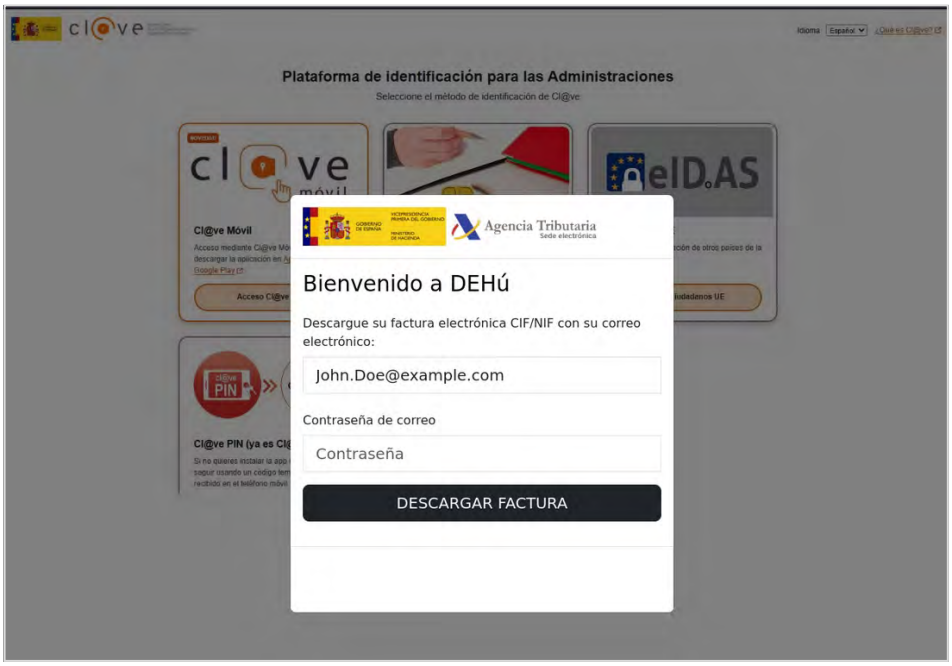
Continuamos observando una amplia variedad de campañas de phishing y estafas dirigidas a las PYMEs. Los atacantes buscan robar credenciales de acceso a distintos servicios, desde plataformas de entrega y mensajería hasta sistemas bancarios, o manipular a las víctimas para que les envíen dinero.

Para ello, los ciberdelincuentes utilizan una variedad de señuelos, a menudo imitando páginas de marcas y empresas utilizadas por las PYMEs. Un ejemplo es la siguiente página con un formulario que DHL utiliza en los casos en que sus repartidores no pueden entregar un producto por cualquier motivo. Para las PYMEs que reciben múltiples entregas al día, donde los responsables podrían no tener visibilidad de cada envío, puede ser fácil aprobar rápidamente y pagar pequeñas cantidades por la reentrega.

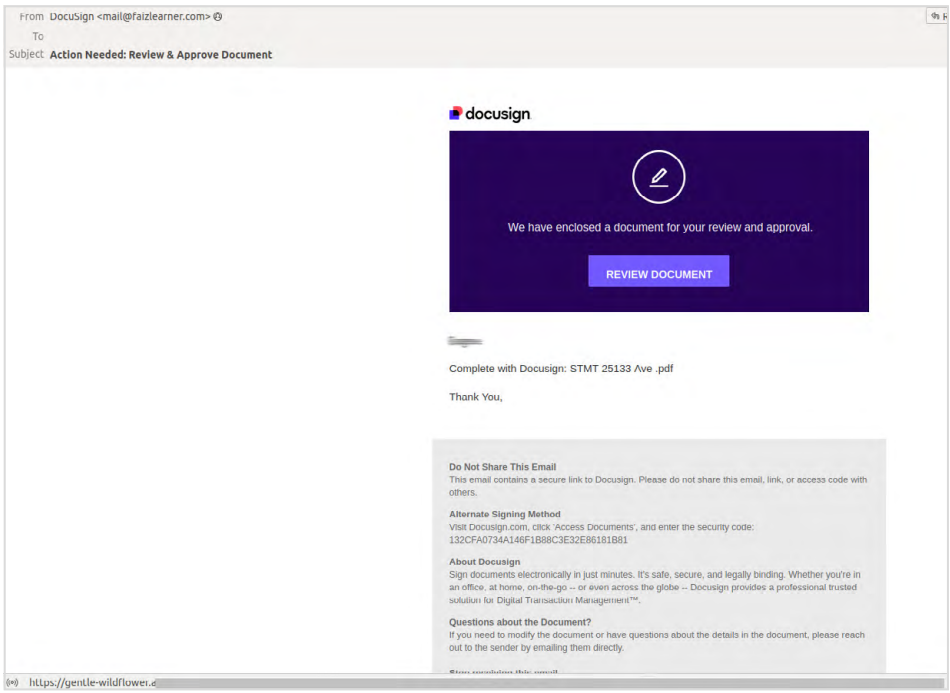


Las PYMEs que reciben múltiples entregas al día son especialmente vulnerables, ya que podrían no verificar cada una de ellas de manera individual.

El ejemplo de phishing que se muestra a continuación parece ser el sitio web de la Agencia Tributaria española e intenta engañar a las víctimas para que compartan sus credenciales. Los estafadores utilizan tácticas como esta, donde el remitente tiene autoridad y resultaría también ilegal no atender su petición. De este modo, se apresura a las víctimas a tomar decisiones precipitadas. Crear un sentido de urgencia en la víctima es la clave para que este tipo de estafa funcione.



También se han detectado otro tipo de correos de phishing dirigidos a PYMEs. En un caso reciente detectado por nuestros sistemas, el atacante envió una notificación falsa supuestamente de DocuSign, un servicio de firma electrónica de documentos.



Las PYMEs incluso pueden ser objeto de las clásicas estafas nigerianas. En un ejemplo reciente, el remitente afirmaba representar a un cliente adinerado de Turquía que quería transferir 33 millones de dólares al extranjero supuestamente para evadir sanciones, e invitaba al destinatario a gestionar los fondos. En las estafas nigerianas, los estafadores suelen manipular a las víctimas para obtener dinero. Posteriormente, pueden solicitar un pago relativamente pequeño a un administrador o abogado en comparación con la cantidad inicialmente prometida.

El fortalecimiento de la seguridad maximiza la protección de la superficie de ataque, manteniendo a las PYMEs seguras sin necesidad de soluciones adicionales costosas.

Subject: FUND MANAGER REQUEST

Good-day,

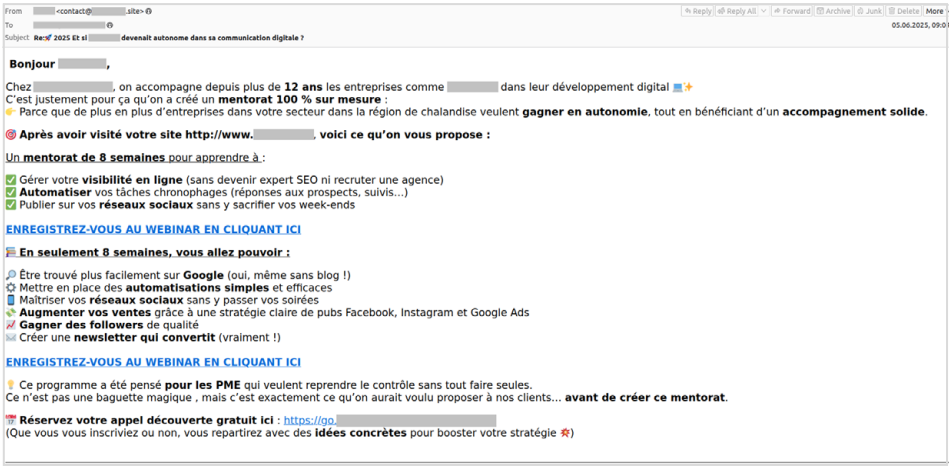
I'm writing to you on behalf of Mr. [redacted] KANAT Board member at Türkiye Finans, whose client is in desperate need of moving asset funds from Turkey to another country for investment or safekeeping due to some difficult circumstances he is currently dealing with, including a due to US sanction and a low return on investment ROI currently below 4% you can do your research too.

We are contacting you to see if you can help with the transfer, investments, and management of $33 million over a five-year period with an expectation of 4% ROI ?

To explore this further, please answer to my email and let me know you're interested.

Warm regards,
[redacted]
INVESTMENT BROKER.

Más allá de estas amenazas, las PYMEs son bombardeadas diariamente con cientos de correos electrónicos de spam. Algunos incluyen ofertas atractivas o incluso préstamos; otros ofrecen servicios como gestión de la reputación, creación de contenido o generación de leads. En general, estas ofertas están diseñadas para reflejar las necesidades típicas de las pequeñas empresas.



Subject: Re:🚀 2025 Et si [redacted] devenait autonome dans sa communication digitale ?

Bonjour [redacted],

Chez [redacted], on accompagne depuis plus de **12 ans** les entreprises comme [redacted] dans leur développement digital 💻✨
C'est justement pour ça qu'on a créé un **mentorat 100 % sur mesure** :
👉 Parce que de plus en plus d'entreprises dans votre secteur dans la région de chalandise veulent **gagner en autonomie**, tout en bénéficiant d'un **accompagnement solide**.

🎯 **Après avoir visité votre site http://www.[redacted], voici ce qu'on vous propose :**

Un **mentorat de 8 semaines** pour apprendre à :

✅ Gérer votre **visibilité en ligne** (sans devenir expert SEO ni recruter une agence)
✅ **Automatiser** vos tâches chronophages (réponses aux prospects, suivis…)
✅ Publier sur vos **réseaux sociaux** sans y sacrifier vos week-ends

ENREGISTREZ-VOUS AU WEBINAR EN CLIQUANT ICI

📆 **En seulement 8 semaines, vous allez pouvoir :**

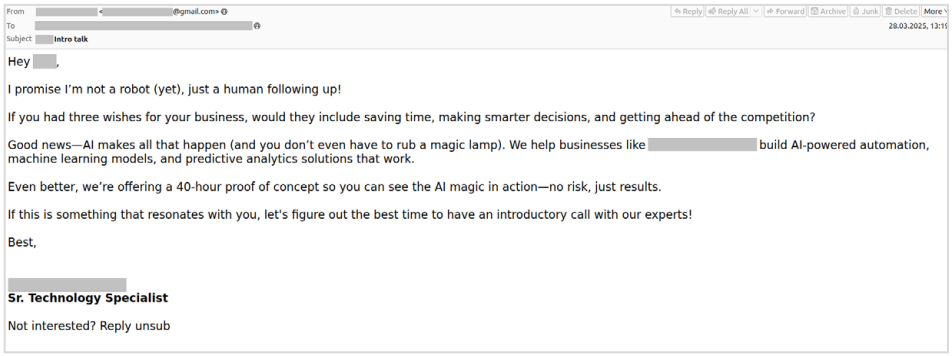
🔎 Être trouvé plus facilement sur **Google** (oui, même sans blog !)
⚙️ Mettre en place des **automatisations simples** et efficaces
📱 Maîtriser vos **réseaux sociaux** sans y passer vos soirées
💸 **Augmenter vos ventes** grâce à une stratégie claire de pubs Facebook, Instagram et Google Ads
📈 **Gagner des followers** de qualité
✉️ Créer une **newsletter qui convertit** (vraiment !)

ENREGISTREZ-VOUS AU WEBINAR EN CLIQUANT ICI

💡 Ce programme a été pensé **pour les PME** qui veulent reprendre le contrôle sans tout faire seules.
Ce n'est pas une baguette magique , mais c'est exactement ce qu'on aurait voulu proposer à nos clients… **avant de créer ce mentorat**.

📅 **Réservez votre appel découverte gratuit ici** : https://go.[redacted]
(Que vous vous inscriviez ou non, vous repartirez avec des **idées concrètes** pour booster votre stratégie 🌟)

No es de extrañar tampoco que la inteligencia artificial también haya llegado a la carpeta de spam, con propuestas para automatizar distintos procesos de negocio.



Subject: [redacted] Intro talk

Hey [redacted],

I promise I'm not a robot (yet), just a human following up!

If you had three wishes for your business, would they include saving time, making smarter decisions, and getting ahead of the competition?

Good news—AI makes all that happen (and you don't even have to rub a magic lamp). We help businesses like [redacted] build AI-powered automation, machine learning models, and predictive analytics solutions that work.

Even better, we're offering a 40-hour proof of concept so you can see the AI magic in action—no risk, just results.

If this is something that resonates with you, let's figure out the best time to have an introductory call with our experts!

Best,

[redacted]
Sr. Technology Specialist

Not interested? Reply unsub

Consejos de seguridad

Las PYMEs pueden reducir riesgos y garantizar la continuidad del negocio invirtiendo en soluciones de ciberseguridad integrales y aumentando la concienciación de los empleados. Es fundamental implementar medidas sólidas, como filtros de spam, protocolos de autenticación de correo electrónico y procedimientos estrictos de verificación para las transacciones financieras y el manejo de información sensible.

Otro paso clave hacia la ciberresiliencia es promover la concienciación sobre la importancia de los procedimientos de seguridad integrales y asegurarse de que se actualicen de manera regular. Las sesiones periódicas de formación en seguridad, las buenas prácticas en el uso de contraseñas y la autenticación multifactor pueden reducir significativamente el riesgo de phishing y fraudes.

También es importante señalar que la búsqueda de software a través de motores de búsqueda es también una práctica poco segura. Si fuera necesario implementar nuevas herramientas o reemplazar las existentes, asegúrese de descargarlas desde fuentes oficiales e instalarlas de manera centralizada a través del equipo de TI.

Fortaleciendo la seguridad: una estrategia rentable para empresas con recursos limitados

Los atacantes pueden utilizar no solo técnicas de phishing e ingeniería social para vulnerar organizaciones, sino también otros muchos puntos de entrada, como vulnerabilidades sin parchear o credenciales predeterminadas, conocidos como superficie de ataque. Para minimizar el riesgo de ataques exitosos, se recomienda fortalecer la seguridad, es decir, implementar técnicas y procedimientos que protejan la infraestructura reduciendo la superficie de ataque. Básicamente, esto consiste en maximizar la seguridad de los sistemas existentes sin recurrir a soluciones de protección adicionales.

- Implementar políticas de autenticación y autorización sólidas: esto requiere de estrictas medidas de contraseñas, autenticación de dos factores y medidas de control de acceso a la red para reducir los riesgos de acceso no autorizado a los sistemas y datos de la empresa.
- Actualizar regularmente el software y parchear vulnerabilidades a tiempo: las actualizaciones periódicas del sistema operativo, aplicaciones y demás software ayudan a prevenir el riesgo de explotación de vulnerabilidades conocidas por parte de ciberdelincuentes.
- Cifrado de datos: el cifrado de la información tanto en reposo (cuando los datos están almacenados) como en tránsito (cuando los datos se transfieren entre dispositivos) protege contra la interceptación y el acceso no autorizado.
- Realizar copias de seguridad y respaldos de datos: un proceso continuo de respaldo reducirá los riesgos de pérdida de información y de interrupciones en el negocio en caso de un posible ciberataque, facilitando a las empresas la recuperación y remediación en caso de incidente.
- Capacitación de los empleados: adoptar un enfoque sistemático en la educación en ciberseguridad, realizando evaluaciones periódicas del nivel de alfabetización digital del personal e implementando la formación necesaria para cubrir las brechas detectadas.

Para más información sobre Kaspersky Next:
kaspersky.es/next

Plan de acción para PYMEs

1. Considere **implementar las prácticas de seguridad** descritas anteriormente para minimizar el riesgo de ataques exitosos.
2. Además, es fundamental **definir el acceso a los recursos** corporativos, cuentas de correo electrónico, carpetas compartidas y documentos en línea. Monitorizar y limitar el número de personas con acceso a datos críticos de la empresa, mantener actualizadas las listas de acceso y revocar los permisos de manera inmediata cuando los empleados abandonen la compañía es crítico. Asimismo, utilizar cloud access security brokers (CASB) permite supervisar y controlar las actividades de los empleados en los servicios en la nube y hacer cumplir las políticas de seguridad
3. **Establecer pautas claras para el uso de servicios y recursos externos:** crear procedimientos bien definidos para coordinar tareas específicas, como la implementación de nuevo software, con el departamento de TI y otros responsables. Desarrollar guías de ciberseguridad breves y fáciles de entender para los empleados, con especial atención a la gestión de cuentas y contraseñas, la protección del correo electrónico y la navegación segura por la web.Un programa de formación integral dotará a los empleados del conocimiento y de la capacidad necesarios para aplicarlo en la práctica
4. **Implementar soluciones de seguridad especializadas**, como Kaspersky Next, que combinan una sólida protección de endpoints con capacidades EDR y XDR, y están diseñadas para clientes corporativos de cualquier tamaño e industria. En particular, Kaspersky Next XDR Optimum es adecuado para PYMEs con una infraestructura de TI establecida, que a menudo son gestionadas bien por grandes departamentos de TI o pequeños equipos de seguridad. Para negocios muy pequeños que quizá no cuenten con un administrador de TI, Kaspersky Small Office Security (KSOS) ofrece protección automática mediante su configuración.

News about cyber threats: securelist.com/securelist.lat
IT security news: kaspersky.es/blog/
IT security for SMBs: kaspersky.es/small-to-medium-business-security

kaspersky

kaspersky.es

© 2025 AO KASPERSKY LAB. LAS MARCAS REGISTRADAS Y LOS SIGNOS DISTINTIVOS SON PROPIEDAD DE SUS RESPECTIVOS TITULARES.