Microsoft es la marca más suplantada (36%) y Mastercard vuelve al ranking de phishing en el quinto puesto (3%)

- **El último Brand Phishing Report del Q1 2025 de Check Point Research revela que Microsoft (36%), Google (12%) y Apple (8%) son las marcas más suplantadas por los ciberdelincuentes.**

Check Point Research, la división de Inteligencia de Amenazas Check Point® Software Technologies Ltd. (NASDAQ: CHKP), pionero y líder global en soluciones de ciberseguridad, ha publicado su último Brand Phishing Report correspondiente al primer trimestre de 2025. Este informe destaca las marcas más suplantadas por los ciberdelincuentes con el objetivo de robar información personal, corporativa y de pago, subrayando la evolución constante de los ataques de phishing en la era digital.

En el primer trimestre de 2025, Microsoft mantuvo su posición como la marca más imitada, representando el 36% de todos los intentos de phishing. Google ascendió al segundo puesto con un 12%, mientras que Apple se mantuvo entre las tres primeras con un 8%. Cabe destacar el regreso de Mastercard al ranking, situándose en la quinta posición, tras no figurar entre las 10 principales desde el tercer trimestre de 2023. El sector tecnológico fue, una vez más, el más suplantado, seguido por las redes sociales y el comercio minorista.

"Los ataques de phishing que se aprovechan de marcas de confianza siguen representando una de las principales amenazas. El regreso de Mastercard a las primeras posiciones pone de relieve el interés de los ciberdelincuentes por suplantar entidades financieras para cometer fraudes. Los consumidores deben extremar la precaución al interactuar con servicios online, especialmente cuando se manejan datos financieros sensibles", explica Omer Dembinsky, director de investigación de datos en Check Point Software.

Principales marcas de phishing en el primer trimestre de 2025

1. Microsoft (36%)

2. Google (12%)
3. Apple (8%)
4. Amazon (4%)
5. Mastercard (3%)
6. Alibaba (2%)
7. WhatsApp (2%)
8. Facebook (2%)
9. LinkedIn (2%)
10. Adobe (1%)

Campaña de phishing dirigida a usuarios de Mastercard

Una de las campañas más destacadas del trimestre fue el incremento de sitios fraudulentos dirigidos a usuarios de Mastercard. En febrero, se detectaron páginas web diseñadas para imitar el sitio oficial de Mastercard, principalmente enfocadas en usuarios de Japón. El objetivo de estos sitios era robar información financiera sensible como números de tarjetas y códigos CVV. Algunos de los dominios identificados fueron:

- mastercard-botan[.]aluui[.]cn
- mastercard-pitiern[.]gmkt6q[.]cn
- mastercard-orexicible[.]bvswu[.]cn
- mastercard-transish[.]gmkt7e[.]cn

Imagen 1. Campaña de phishing de Mastercard

Aunque estos dominios ya no están activos, su proliferación subraya el interés de los ciberdelincuentes por suplantar instituciones financieras, y recuerda a los usuarios la importancia de verificar la legitimidad de las plataformas con las que interactúan en operaciones financieras.

Página falsa de inicio de sesión de OneDrive: ejemplo de suplantación de identidad

Otra campaña significativa detectada este trimestre involucró la creación de una página falsa de inicio de sesión que imitaba OneDrive de Microsoft. El dominio fraudulento login[.]onedrive-micrasoft[.]com fue diseñado para replicar el aspecto del portal oficial de Microsoft, con el fin de engañar a los usuarios para que introdujeran sus credenciales, incluidos correos electrónicos y contraseñas. Esta táctica muestra cómo los ciberdelincuentes siguen perfeccionando el uso de páginas de apariencia legítima para comprometer la seguridad de los usuarios.

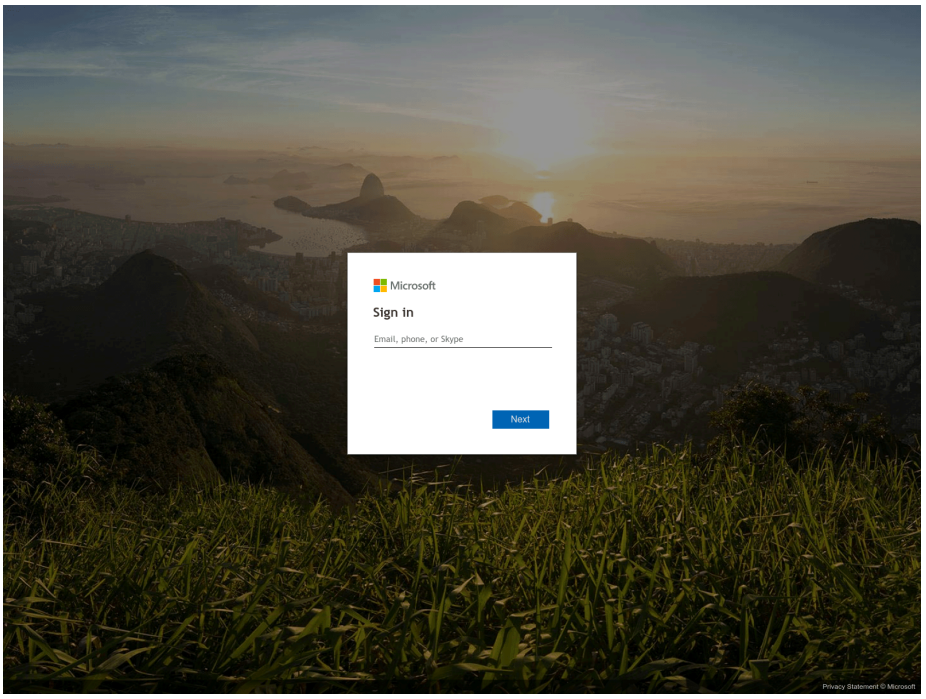

Imagen 2. Login[.]onedrive-micrasoft[.]com

Tendencias del sector: el auge de los ataques al sector tecnológico

El sector tecnológico volvió a ser el más afectado por ataques de phishing en el primer trimestre de 2025. A medida que tanto empresas como consumidores confían cada vez más en servicios digitales y en la nube, estas plataformas se convierten en objetivos recurrentes para los atacantes. Empresas como Microsoft, Google y Apple fueron las más imitadas, aunque también se observaron ataques dirigidos a plataformas de redes sociales como Facebook, LinkedIn y WhatsApp, así como a grandes sitios de comercio electrónico como Amazon.

Acerca de Check Point Research

Check Point Research proporciona inteligencia sobre ciberamenazas a los clientes de Check Point Software y a la comunidad de inteligencia. El equipo de investigación recopila y analiza datos de ciberataques globales almacenados en ThreatCloud para mantener los ciberdelincuentes a raya, al tiempo que se asegura de que todos los productos de Check Point estén actualizados con las últimas protecciones. El equipo de investigación está formado por más de 100 analistas e investigadores que cooperan con otros proveedores de seguridad, las fuerzas de seguridad y varios CERTs.

Acerca de Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. es un proveedor líder de soluciones de ciberseguridad para empresas y gobiernos de todo el mundo. La cartera de soluciones de Check Point Infinity protege a las empresas y organizaciones públicas de los ciberataques de 5ª generación con una tasa de captura líder en la industria de malware, ransomware y otras amenazas. Infinity se compone de cuatro pilares fundamentales que ofrecen una seguridad sin compromisos y una prevención de amenazas de quinta generación en todos los entornos empresariales: Check Point Harmony, para usuarios remotos; Check Point CloudGuard, para proteger automáticamente los entornos cloud; y Check Point Quantum, para proteger los perímetros de la red y los centros de datos, todo ello controlado por la gestión de seguridad

unificada más completa e intuitiva de la industria; Check Point Horizon, una suite de operaciones de seguridad que da prioridad a la prevención. Check Point Software protege a más de 100.000 organizaciones de todos los tamaños.

Aviso legal sobre declaraciones prospectivas

Este comunicado de prensa contiene declaraciones prospectivas. Las declaraciones prospectivas generalmente se refieren a eventos futuros o a nuestro desempeño financiero u operativo futuro. Las declaraciones prospectivas incluidas en este comunicado de prensa incluyen, pero no se limitan a, declaraciones relacionadas con nuestras expectativas respecto al crecimiento futuro, la expansión del liderazgo de Check Point Software en la industria, la mejora del valor para los accionistas y la entrega de una plataforma de ciberseguridad líder en la industria a clientes de todo el mundo. Nuestras expectativas y creencias sobre estos temas pueden no materializarse, y los resultados o eventos futuros están sujetos a riesgos e incertidumbres que podrían hacer que los resultados reales o los eventos difieran significativamente de los proyectados.

Las declaraciones prospectivas contenidas en este comunicado de prensa también están sujetas a otros riesgos e incertidumbres, incluyendo aquellos descritos con mayor detalle en nuestros archivos ante la Comisión de Bolsa y Valores (SEC), incluyendo nuestro Informe Anual en el Formulario 20-F presentado ante la SEC el 2 de abril de 2024. Las declaraciones prospectivas en este comunicado de prensa se basan en la información disponible para Check Point Software a la fecha de este documento, y Check Point Software renuncia a cualquier obligación de actualizar cualquier declaración prospectiva, salvo que lo exija la ley.

Brand Partners PR
Valeria Bin Calvar
Cel. +54 11 2651-0686
valeria@brand-partners.com.ar