ENTHEC

WHITEPAPER

PROTECCIÓN DE MARCA:

Campañas de phishing, fraude y scam en redes sociales

kartos
XTI watchbots

kartos
XTI watchbots

Índice

PAG.

INTRODUCCIÓN

En la era digital, las redes sociales se han convertido en una parte integral de nuestras vidas y de los negocios, brindando oportunidades para conectarse, compartir contenido e interactuar con diversas comunidades, entre las que se encuentran los clientes.

Sin embargo, esta creciente dependencia también ha dado lugar a un aumento en las campañas de phishing, fraude y scam en estos entornos virtuales. Estas prácticas delictivas han evolucionado, incluyendo la usurpación de identidad corporativa para engañar a usuarios y clientes y obtener información confidencial o un enriquecimiento ilícito.

En este documento, exploraremos el gran problema que para las organizaciones suponen las campañas de phishing, fraude y scam con usurpación de identidad corporativa en redes sociales, proporcionando datos sobre las técnicas utilizadas por los ciberdelincuentes, las consecuencias para las organizaciones de este tipo de cibercrimen y ofreciendo estrategias de prevención y protección frente a estas ciberamenazas en constante evolución.

¿QUÉ SON EL PHISHING, EL FRAUDE Y EL SCAM Y CÓMO SE HAN ADAPTADO A LAS REDES SOCIALES?

El phishing es un método utilizado por los ciberdelincuentes para obtener información confidencial, como contraseñas o detalles de tarjetas de crédito, haciéndose pasar por una entidad legítima.

En el contexto de las redes sociales, los estafadores utilizan técnicas sofisticadas para enviar mensajes directos o publicaciones que aparentan ser de una organización o institución reconocidas. Los ciberdelincuentes han adaptado estas tácticas al entorno de las redes sociales, aprovechando la confianza y familiaridad que los usuarios tienen con estas plataformas.

Además del phishing, los ciberdelincuentes también utilizan las redes sociales para llevar a cabo campañas de fraude y scam. Estas actividades ilegales incluyen la venta de productos falsificados, promociones engañosas, esquemas de inversión fraudulentos y mucho más.

Para llevar a cabo estas campañas de phishing, fraude y scam en redes sociales, los ciberdelincuentes se valen de la usurpación de identidad corporativa. Los estafadores se hacen pasar por marcas reconocidas o marcas específicas sobre las que tienen algún interés, utilizando logotipos, imágenes y mensajes similares a los utilizados por las empresas legítimas.

kartos
XTI watchbots

LA USURPACIÓN DE LA IDENTIDAD CORPORATIVA EN REDES SOCIALES: UNA AMENAZA EN CONSTANTE EVOLUCIÓN

La usurpación de la identidad corporativa, también conocida como abuso de marca, en redes sociales abarca una variedad de tácticas que van desde perfiles falsos que se hacen pasar por la marca hasta la distribución de contenido malicioso bajo el nombre de la misma. Esto puede terminar provocando daños significativos para la reputación y la confianza del público en la marca. Además, puede abrir la puerta a posibles fraudes y estafas, desencadenando consecuencias financieras graves.

FALSIFICACIÓN DE PERFILES

Los ciberdelincuentes crean perfiles falsos que imitan a la marca genuina, utilizando nombres y logotipos similares. Estos perfiles a menudo se utilizan para difundir información falsa, promover productos fraudulentos o, incluso, estafar al cliente.

PHISHING A TRAVÉS DE REDES SOCIALES

Se aprovechan de la familiaridad que las personas tienen con ciertas marcas para enviar mensajes de phishing. Estos mensajes pueden contener enlaces maliciosos o solicitudes de información confidencial, engañando a los usuarios desprevenidos.

PUBLICACIÓN DE CONTENIDO MALICIOSO

Los atacantes comparten enlaces o archivos infectados bajo el nombre de la marca, aprovechando la confianza que los seguidores tienen en ella. El fin es la propagación de malware o la exposición a contenido perjudicial.

SUPLANTACIÓN DE SERVICIOS

Se crean cuentas que se hacen pasar por el servicio al cliente de la marca, respondiendo a consultas legítimas y, a menudo, direccionando a los usuarios hacia sitios falsos o peligrosos.

ANALIZANDO EL IMPACTO: CONFIANZA DEL CLIENTE Y REPUTACIÓN DE LA MARCA

El abuso de marca en redes sociales comprende una variedad de estratagemas, desde la creación de perfiles falsos hasta la difusión de contenido malicioso bajo el paraguas de la marca afectada. Este ciberdelito en rápida evolución ha adquirido una complejidad que exige una respuesta igualmente sofisticada por parte de las organizaciones, ya que acarrea consecuencias muy graves:

- **Erosión de la confianza del cliente:** El abuso de marca tiene un impacto directo en la confianza de los clientes. Cuando los usuarios son expuestos a perfiles falsos o contenido malicioso bajo el nombre de una marca legítima, se desencadena una crisis de confianza. La confusión y el escepticismo se apoderan de los seguidores y clientes, lo que puede resultar en una disminución en el compromiso y, en última instancia, en las ventas.
- **Reputación de la marca en riesgo:** La reputación de una marca es uno de sus activos más valiosos. El abuso de marca o usurpación de la identidad corporativa en redes sociales puede dañar irreparablemente esta reputación. Las actividades maliciosas, como la difusión de información falsa o la promoción de productos fraudulentos bajo el nombre de una marca, desencadenan una cascada de efectos reputacionales negativos.
- **Impacto financiero y legal:** Más allá de los efectos reputacionales y de confianza, el abuso de marca puede tener implicaciones financieras y legales significativas. Las marcas pueden incurrir en pérdidas directas debido a la disminución de las ventas y los costos asociados con la gestión de crisis de reputación. Además, en casos graves, el abuso de marca puede dar lugar a litigios y sanciones regulatorias.

LOS LÍMITES DE LA EDUCACIÓN Y LA CONCIENCIACIÓN

Educar y concienciar al usuario y cliente sobre este tipo de cibercrimen con el fin de que adquieran habilidades para esquivar el engaño es la parte principal de las estrategias que las organizaciones suelen adoptar en la lucha contra la usurpación de la identidad corporativa. Sin embargo, en el entorno digital actual, la protección de una marca requiere un enfoque holístico. Si bien la educación y concienciación de la audiencia son piedras angulares, no pueden ser la única línea de defensa.

El abuso de marca en redes sociales abarca desde la creación de perfiles falsos hasta la distribución de contenido malicioso bajo la identidad de una marca legítima. Este fenómeno se ha vuelto cada vez más sofisticado y peligroso, lo que exige una respuesta proactiva de identificación y eliminación que vaya más allá de los límites de la educación y concienciación de usuarios y clientes.

SOFISTICACIÓN DE LOS ATAQUES

Los ciberdelincuentes han perfeccionado sus técnicas. Ahora emplean ingeniería social de alta complejidad, lo que significa que incluso usuarios y clientes bien informados pueden caer en trampas cuidadosamente diseñadas.

FALSA SENSACIÓN DE SEGURIDAD

A pesar de una formación adecuada, los usuarios y clientes pueden desarrollar una falsa sensación de seguridad, creyendo que están exentos de ser engañados. Esto puede llevar a una disminución de la vigilancia y a una mayor susceptibilidad a los ataques.

NUEVAS FORMAS DE ATAQUE

Los atacantes están constantemente innovando. La introducción de técnicas como la suplantación de identidad asistida por inteligencia artificial presenta un desafío adicional para la educación y concienciación de la audiencia.

IMPACTO EN LA CONFIANZA DE LA MARCA Y COMUNICACIONES REALES DE LA ORGANIZACIÓN

La educación y concienciación son herramientas vitales en la lucha contra ciberamenazas. Sin embargo, un enfoque unilateral puede tener consecuencias colaterales no deseadas:

- Impacto en la confianza de la marca por la percepción de vulnerabilidad de la organización. Esta percepción puede llevar a una disminución de la confianza en la capacidad de la marca para proteger sus activos digitales.
- Disminución del seguimiento e impacto las campañas de comunicación reales e importantes de marca:

-Confusión entre los mensajes de Ciberseguridad y los de marca: Una educación excesiva en ciberseguridad puede eclipsar las comunicaciones de marca genuinas.

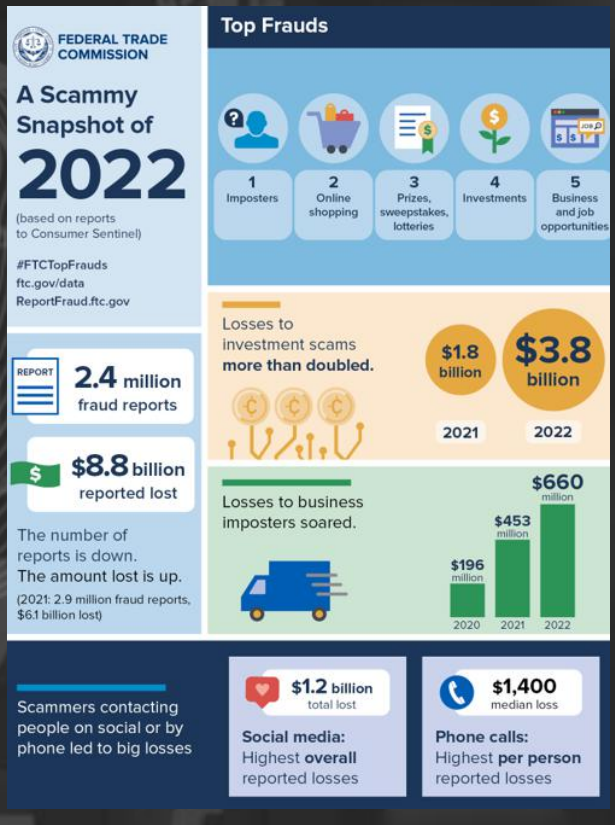
-Pérdida de enfoque en la Misión de la marca: Cuando la educación en Ciberseguridad se vuelve dominante, la misión y valores de la marca pueden perderse en el ruido. Esto puede llevar a una falta de cohesión y dirección en la estrategia de comunicación de la marca.

-Desconfianza de cualquier comunicación de la marca que no sea sobre Ciberseguridad: Paradójicamente, cuando la educación y la concientización son la piedra angular de la estrategia, se produce el efecto contra el que se intenta luchar la erosión en la confianza de las comunicaciones de la marca que no traten sobre Ciberseguridad. En la práctica, esto significa que las campañas comerciales, publicitarias, de captación o fidelización de la organización son cada vez menos eficaces, porque al destinatario le cuesta confiar en el contenido, mientras que aquellas que tratan sobre un tema ajenos al negocio, la Ciberseguridad, son las únicas en las que obtienen confianza plena.

DATOS:

Según datos de la Comisión Federal de Comercio de EEUU (Federal Trade Commission, FTC) los consumidores estadounidenses informaron haber perdido casi $8.8 mil millones por fraude en 2022, un aumento de más del 30% con respecto al año anterior.

Las pérdidas por fraude a través de las plataformas de redes sociales ascendieron a 1.200 millones de dólares en 2022.



¿Puede una Marca sentirse tranquila cuando su estrategia de lucha contra la usurpación de su identidad en redes sociales se basa principalmente en decirle a seguidores y clientes que desconfíen de cualquier mensaje en el que aparezca su marca por verosímil que resulte?

¿Es esta una estrategia realmente alineada con los intereses de la organización?

¿Acaso no es una estrategia que termina teniendo el efecto que se intenta evitar?

kartos
XTI watchbots

CONSECUENCIAS DE LA SUPLANTACIÓN DE LA IDENTIDAD CORPORATIVA EN LAS REDES SOCIALES

- **Pérdidas financieras:** la suplantación de la identidad corporativa puede generar pérdidas financieras para las empresas, tanto en forma de pérdida de ventas como en multas.
- **Daño a la reputación:** La suplantación de la identidad corporativa en las redes sociales daña la reputación de una organización y de su marca. Los estafadores pueden utilizan la marca de la empresa para difundir información falsa o participar en comportamientos poco éticos, e, incluso, delictivos cuyos efectos negativos alcanzan a la imagen de la organización.
- **Pérdida de confianza del cliente:** Tras una campaña de phishing, fraude o scam con en redes sociales, los clientes pasan a desconfiar de la interacción con la organización en las redes sociales al percibir que no toma medidas para proteger su marca.
- **Problemas legales:** La suplantación de identidad corporativa puede acarrear problemas legales cuando los estafadores utilizan la marca para participar en actividades ilegales, ya que la organización puede inicialmente ser considerada responsable hasta que demuestre la suplantación.

¿CÓMO AFECTA LA SUPLANTACIÓN DE IDENTIDAD CORPORATIVA EN LAS REDES SOCIALES A LA LEALTAD DEL CLIENTE Y A LA REPUTACIÓN DE MARCA?

- **Pérdida de confianza:** Si los clientes creen que la empresa no está tomando las medidas adecuadas para proteger su marca, desconfían de la interacción con la empresa en las redes sociales.
- **Confusión:** Si los clientes no pueden distinguir entre las cuentas oficiales de redes sociales de la organización y las cuentas falsas, pueden confundirse con los mensajes y las ofertas de la empresa.
- **Imagen de marca negativa:** Si los ciberdelincuentes utilizan la marca de la empresa para difundir información falsa o participar en un comportamiento poco ético, la imagen queda dañada.
- **Disminución de la interacción:** La suplantación de identidad corporativa conduce a una disminución de la participación en las redes sociales. Si los clientes no están seguros de la autenticidad de las cuentas de redes sociales de la organización, es menos probable que interactúen con ella.
- **Disminución de la lealtad:** La suplantación de identidad corporativa conduce a una progresiva disminución de la lealtad del cliente. Si los clientes sienten que la organización no está tomando las medidas adecuadas para proteger su marca, es menos probable que permanezcan leales a ella.

¿CUÁLES SON ALGUNOS DE LOS RIESGOS FINANCIEROS ASOCIADOS CON LA SUPLANTACIÓN DE IDENTIDAD CORPORATIVA EN LAS REDES SOCIALES?

- **Pérdida de ingresos:** La suplantación de identidad corporativa e las redes sociales puede suponer una pérdida de ingresos para las empresas por la pérdida de ventas a clientes engañados o estafados.
- **Honorarios legales:** La suplantación de identidad corporativa puede dar lugar a honorarios legales para las organizaciones cuando los ciberdelincuentes utilizan la identidad corporativa para participar en actividades ilegales, lo que obliga a la organización a emprender acciones legales para proteger su marca.
- **Daño al valor de la marca:** Los ciberdelincuentes utilizan la marca para participar en campañas de phishing, fraude o scam o difundir información falsa, dañando la imagen y la reputación, lo que conlleva una disminución del valor de la marca.
- **Costo de recuperación de la confianza de marca:** Después de una suplantación de identidad corporativa en redes sociales exitosa por parte de la ciberdelincuencia, la organización se ve obligada a invertir en potentes campañas de comunicación para recuperar parte de la confianza de marca perdida.

ERRORES COMUNES DE LAS ORGANIZACIONES A LA HORA DE EVITAR EL ABUSO DE MARCA EN LAS REDES SOCIALES

- **No monitorizar las redes sociales**: No monitorizar de forma continua las redes sociales para detectar el uso fraudulento de su identidad corporativa permite a los estafadores utilizar con impunidad la marca para engañar a los clientes.
- **No tener una estrategia de protección proactiva**: Cuando una organización no tiene establecida una estrategia proactiva de protección de su marca en redes sociales, que prevenga y neutralice las campañas, se vuelve vulnerable a ser utilizada para ataques de phishing y otros tipos de fraude.
- **No estar activas en redes sociales:** No tener perfiles en redes sociales o tenerlos, pero inactivos, propicia que los perfiles falsos creados por los ciberdelincuentes puedan tener una mayor credibilidad ante los clientes y usuarios.
- **No proteger la marca con estrategias y tecnologías avanzadas:** La sofisticación de los ciberataques hace necesaria una protección de la organización que esté a la altura y utilice estrategias avanzadas y tecnologías como la Inteligencia Artificial y la automatización para poder dar las respuestas necesarias en el momento preciso.

ESTRATEGIAS DE DEFENSA AVANZADAS PARA EVITAR ESOS ERRORES EN LA PROTECCIÓN DE LA MARCA

- **Herramientas de Ciberinteligencia para la detección y prevención avanzadas:** La inversión en herramientas de Ciberinteligencia y detección de última generación es esencial. Las soluciones basadas en inteligencia artificial y aprendizaje automático identifican los perfiles falsos y las actividades maliciosas de manera más efectiva y rápida que los métodos tradicionales y son capaces de realizar el seguimiento automático de las campañas fraudulentas activas o latentes en redes sociales hasta su total eliminación.
- **Análisis de comportamiento y patrones de ataque**: Entender los patrones de comportamiento de los atacantes es crucial. La monitorización constante y el análisis de datos pueden revelar tendencias emergentes y permitir respuestas proactivas.
- **Estrategias de respuesta y recuperación rápidas**: Es esencial contar con una estrategia de respuesta bien definida ante la detección de la usurpación de la identidad corporativa en campañas de phishing, fraude o scam en redes sociales. La capacidad de detección rápida y de respuesta limita el daño a la marca.
- **Colaboración con plataformas de redes sociales**: Resulta crucial contar con la capacidad de informar de inmediato a las plataformas de redes sociales sobre cuentas falsas o actividades sospechosas y trasladar los datos esenciales para acelerar la respuesta y la eliminación de los perfiles fraudulentos.

AMENAZAS SOBRE LA MARCA QUE LAS SOLUCIONES DE SOFTWARE DE CIBERINTELIGENCIA AYUDAN A PREVENIR

- **Productos falsificados**: Detección de sitios con productos falsificados y vendedores no autorizados.
- **Estafas en línea**: Monitorización de redes sociales, mercados en línea y sitios web en busca de campañas de phishing, fraude y scam con utilización fraudulenta de la identidad corporativa.
- **Daño a la reputación**: Monitorización de las redes sociales en busca de actividades fraudulenta causantes de daños a la reputación.
- **Infracción de marca registrada**: Monitorización de los registros de dominio para detectar cualquier uso fraudulento y eliminar sitios web fraudulentos rápidamente.
- **Uso no autorizado de imágenes de marca:** Utilización de herramientas avanzadas de reconocimiento de imágenes y logotipos para encontrar cuentas falsas que utilicen la identidad corporativa.
- **Uso no autorizado de la propiedad intelectual de la organización**: Monitorización de las redes sociales para la detección de cualquier uso indebido de la propiedad intelectual, utilizando algoritmos avanzados para escanear Internet y las plataformas de redes sociales.
- **Ciberataques**: Detección y prevención de ciberataques, incluidos los ataques de phishing y el malware.

CAPACIDADES CLAVE DE LAS SOLUCIONES DE CIBERINTELIGENCIA PARA LA PROTECCIÓN DE MARCA EN REDES SOCIALES

- **Monitorización de la Clear Web, Deep Web y Dark Web incluyendo las redes sociales:** El software debe proporcionar monitorización y registros automatizados para los equipos legales y de cumplimiento, lo que ayuda a garantizar que la marca esté representada correctamente en la web. Esto incluye el monitorización de plataformas de redes sociales, mercados en línea y sitios web en busca de productos falsificados o infracciones de marcas comerciales.
- **Monitorización y eliminación de registros de dominios y subdominios:** El software debe monitorizar los registros de dominios para detectar cualquier uso fraudulento de la marca. También debe ser capaz de detectar sitios web fraudulentos rápidamente.
- **Detección de dominios y cuentas similares, pero no iguales a los oficiales:** La herramienta de Ciberinteligencia debe ser capaz de detectar dominios, subdominios y cuentas que no sean iguales, pero sí muy similares a los oficiales, ya sea porque contienen pequeños y casi indetectables errores tipográficos, ligeros cambios en el diseño o una redacción extraña.
- **Seguimiento, alarmas e informes con datos precisos en tiempo real:** El software debe registrar datos automáticamente y emitir alarmas de detección de abuso de marca en tiempo real, así como proporcionar los informes necesarios para que la organización pueda respandar las denuncias ante las plataformas y conseguir la eliminación d eperfiles y campañas fraudulentas.

BENEFICIOS DE UTILIZAR SOLUCIONES DE CIBERINTELIGENCIA CON CAPACIDADES DE DETECCIÓN DEL ABUSO DE MARCA EN REDES SOCIALES

- Mantener la integridad de la marca: Gracias a la detección en tiempo real del uso no autorizado o fraudulento de la marca.
- Gestionar la reputación online: Gracias a la monitorización constante de las redes sociales, mercados online y sitios web en busca de usurpación de marca.
- Aumentar la confianza de los clientes: Al prevenir el uso fraudulento de la identidad corporativa, las empresas aumentan la confianza y la lealtad de los clientes, demostrando que llevan a cabo una estrategia de protección proactiva que no traspasa la responsabilidad a sus clientes o seguidores.
- Reducir las posibles pérdidas de ingresos: Gracias a la detección y eliminación de cuentas abiertas para realizar falsificaciones y fraudes.
- Garantizar una imagen de marca coherente y positiva: Mediante la detección, denuncia y eliminación de sitios web y cuentas de redes sociales fraudulentos.
- Detectar webs y cuentas suplantadoras: Permite a las organizaciones tomar medidas para denunciar la suplantación ante las plataformas de redes sociales, pedir su borrado y destruir la amenaza.
- Detectar campañas de phishing, fraude y scam con usurpación de la identidad corporativa: Evita que los clientes y usuarios sean víctimas de este tipo de campañas y refuerza su confianza en la marca.
- Rastrear la fuente de la infracción: Seguimiento y detección de la fuente de la infracción para tomar las medidas necesarias para eliminar la amenaza, incluida la denuncia de estafas en línea y el monitoreo de las redes sociales para detectar daños a la reputación.
- Seguimiento, alarmas e informes precisos en tiempo real: Recepción de datos y análisis en tiempo real de la usurpación de la identidad corporativa en redes sociales para campañas de phishing, fraude o scam, con el objetivo de desactivarlas antes de que puedan llegar a los clientes y usuarios y tener éxito.

kartos®
XTI watchbots

EASM + DRPS + SRS

EN UNA SOLA PLATAFORMA

Kartos XTI Watchbots es la plataforma de ciberinteligencia desarrollada por Enthec para extender el perímetro de seguridad controlado por las organizaciones. Concebida desde un enfoque de estrategia hacker, Kartos está en permanente proceso de I+D para incorporar categorías y capacidades adelantadas a la evolución de los ciberataques.

Capa de IA que permite el funcionamiento 100% automatizado sin intervención humana en ninguna parte del proceso.

Funcionamiento continuo 365x24x7, lo que permite detectar filtraciones de nueva información prácticamente en tiempo real.

Herramienta estrictamente no intrusiva. La investigación se realiza en Internet, la Deep Web y la DarkWeb y no se ataca el perímetro IT de las organizaciones, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.

Máxima sencillez de uso. No requiere ninguna configuración compleja. Basta con introducir el dominio en la plataforma y funciona de manera autónoma, sin necesidad de configurar parámetros de búsqueda ni de cualquier otro criterio de localización de información.

Única plataforma que analiza las conversaciones en redes sociales desde la perspectiva de detección de amenazas y ataques, más allá de la relativa a reputación y branding.

Monitorización automatizada, objetiva y continúa de los riesgos causados por las terceras partes que pertenecen a la Superficie de Ataque Externa de la organización.

EXTERNAL ATTACK SURFACE MANAGEMENT

Detección de activos corporativos e información sobre sistemas, servicios en la nube y aplicaciones que están disponibles y visibles en el dominio público para cualquier ciberdelincuente.

DIGITAL RISK PROTECTION SERVICES

Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar a cabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la organización.

SECURITY RATING SERVICES

Evaluación independiente de riesgos propios y de terceros, para una visualización amplia de la madurez en ciberseguridad de cualquier organización utilizando un enfoque externo. Ampliación y ponderación de la información proporcionada por los métodos tradicionales de evaluación de riesgos por terceros.

Análisis de 9 Categorías de Amenazas

- Red
- Salud de DNS / Phishing
- Gestión de Parches
- Reputación IP
- Seguridad Web
- Seguridad e-mail
- Filtración de Documentos
- Filtración de Credenciales
- Redes Sociales

Conoce más sobre nuestras licencias. Prueba de forma gratuita la Ciberinteligencia XTI. Empieza a usar Kartos.

hello@enthec.com

#AlwaysWatching

ENTHEC

@enthec

@enthecsolutions

@enthecsolutions

kartos
XTI watchbots