CERVIERI MONSUAREZ

PHISHING: casos reales y como combatirlo.

Concepto

El “Phishing” es el acto ilícito de suplantar la identidad de una persona o empresa a fin de recabar información y datos personales de los usuarios de internet.

El Phishing se lleva adelante mediante actos de ingeniería social, los cuales se definen como *“una de las formas en las que los cibercriminales usan las interacciones entre personas para que el usuario comparta información confidencial. Ya que la ingeniería social se basa en la naturaleza humana y las reacciones humanas, hay muchas formas en que los atacantes pueden engañar, en línea o sin conexión[1]”.*

Busca afectar directamente a los usuarios de internet, al recabar de forma ilegitima sus datos personales para poder venderlos a terceras empresas, o recabar datos e información de los usuarios para estafas y lograr un perjuicio económico en contra de los usuarios.

Los ataques de Phishing también pueden afectar directamente derechos de la empresa o persona física que está siendo suplantada, al emplear sus signos distintivos para generar confusión en los usuarios. Mediante el uso de marcas, imágenes de productos, o directamente la imitación de los sitios web oficiales, los phishers (individuos responsables de los ataques de phishing) buscan inducir en confusión a los usuarios de que se tratan de páginas oficiales o respaldadas por las empresas cuyas marcas utilizan, para así sustraer su información personal.

Esto también puede llevar a que, al momento de ser víctima de phishing, los usuarios busquen respuestas o soluciones con las empresas cuyas marcas figuraban en el sitio malicioso.

1. https://lam.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

Identificación y baja de sitios

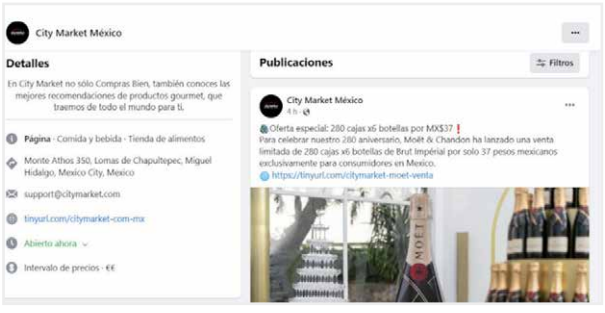
En Cervieri Monsuarez, contamos con un área especializada que se dedica a detectar y combatir estos sitios maliciosos. La finalidad de identificar y dar de baja estos sitios de forma celera, es que los mismos estén activos por el menor tiempo posible, y así evitar que el problema escale y se genere un posible daño al consumidor y a la empresa cuyos derechos de propiedad intelectual e industrial están siendo violados.

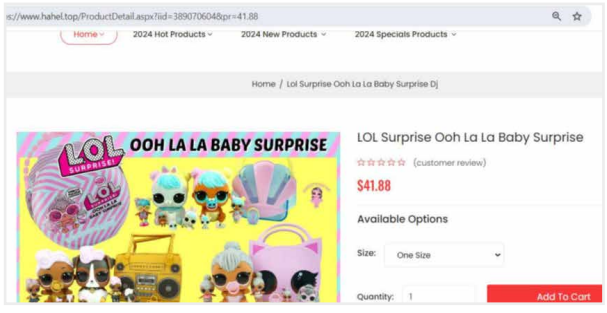
Al detectar los sitios maliciosos, o si el cliente nos informa de un posible sitio, realizamos una investigación del sitio para determinar donde se encuentra alojado, si posee más sitios vinculados, y recabar de esta forma toda la información posible para tomar las medidas pertinentes. Una vez se cuenta con la información necesaria, se proceden a tomar las medidas legales, trabajando en conjunto con nuestro equipo de IT, para lograr la baja de los sitios maliciosos.

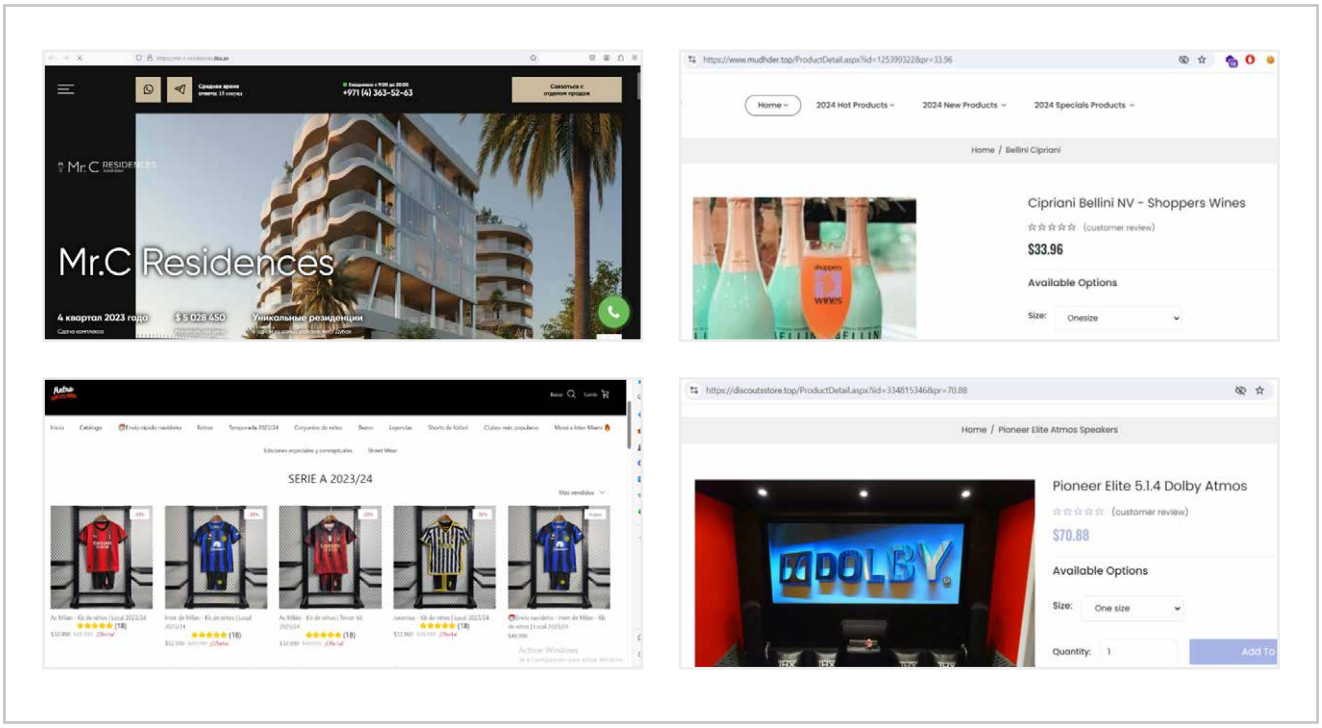
Casos de Phishing

Hoy en día, podemos ver que los casos de Phishing han mutado ampliamente, pasando de ser el típico caso de recibir un correo de un banco con el mensaje “actualice su contraseña” o un mensaje de texto indicando que “te ha llegado un paquete” a encontrar intentos de Phishing utilizando todo tipo de marcas, desde tiendas online de venta de bebidas alcohólicas, hotelería, sorteos, etc. Todos estos casos tienen en común el uso por parte del phisher de marcas y nombres reconocidos por los usuarios, para hacerlos caer en el engaño a costas de la confianza y la reputación de las marcas afectadas.

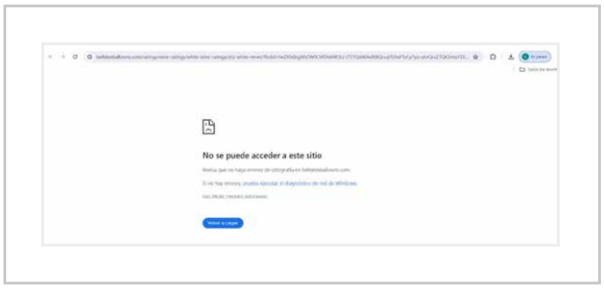
Estas nuevas modalidades se caracterizan con contar con un sitio madre alojado en un dominio determinado, y luego ramificar los diferentes sitios relacionados en otros subdominios, haciendo más difícil la localización de la totalidad de los sitios maliciosos. A continuación, podemos ver algunos ejemplos de sitios maliciosos, los cuales tras un análisis pudimos determinar que se trataban de sitios de phishing:







Medidas que se llevaron a cabo



En todos los casos mencionados, se procedió a analizar el sitio web donde se realizaban los actos de suplantación en internet, y habiendo identificados tanto el sitio inicial como todos los sitios relacionados, se procedió a la denuncia de cada sitio ante las distintas plataformas en donde el enlace estaba siendo compartido.

Luego de varias comunicaciones con las correspondientes áreas legales de las plataformas en cuestión, todos los sitios fueron retirados no solo de los buscadores, sino que los mismos ya no se encuentran disponibles para su ingreso.

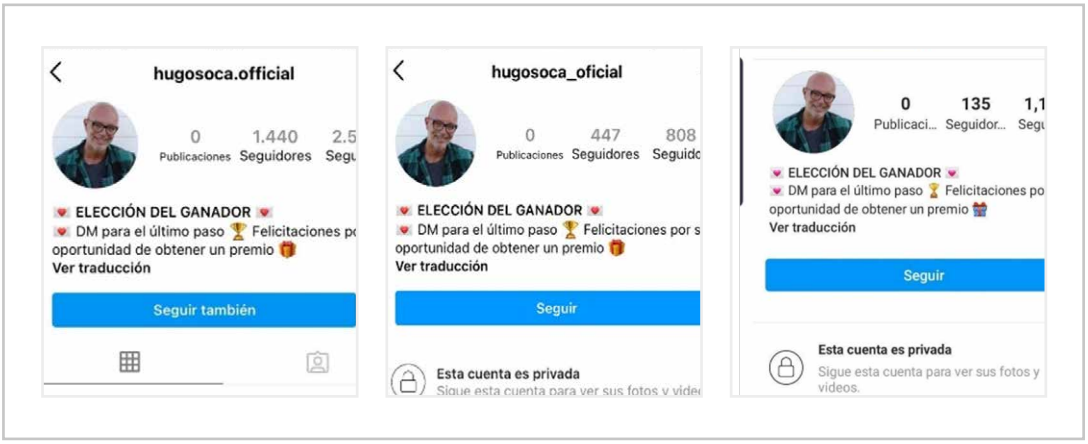
Phishing por suplantación de identidad

Otra de las modalidades de phishing es la suplantación de la identidad de una persona, con el fin de recabar información y datos personales de los usuarios de internet.

Un caso relevante de esta índole fue el del cocinero Uruguayo Hugo Soca. En este caso, se crearon múltiples perfiles de Instagram pretendiendo suplantar la identidad del reconocido Chef Hugo Soca, los cuales se contactaban

con los participantes del sorteo que el Sr. Soca estaba llevando adelante en su perfil, solicitando números de tarjetas de crédito con la excusa de que eran los ganadores del mismo y de esta forma lograr hacerse de esos datos para luego usarlos en su beneficio.

En el presente caso, presentamos denuncia penal en la Fiscalía e investigación por parte de Delitos Informáticos de INTERPOL a los efectos de solicitarle a Instagram la baja del perfil a los efectos de evitar que ese perfil confunda a los consumidores.



Uruguay a la vanguardia de los delitos informáticos

Es importante destacar que este año se aprobó en Uruguay la Ley N° 20.327 “REGULACION PARA LA PREVENCION Y REPRESION DE LA CIBERDELINCUENCIA”, que modifica el Código Penal Uruguayo, tipificando múltiples delitos informáticos[2], entre ellos el delito de Fraude Informático y Suplantación de identidad:

Fraude informático: El que con estratagemas induzca en error a alguna persona para obtener información mediante tecnologías de la información con un fin de aprovechamiento injusto, el que efectué manipulaciones informáticas con la finalidad de realizar operaciones financieras en perjuicio de otro.

Suplantación de identidad: El que usurpe, adopte, cree o se apropie de una identidad de otra persona jurídica o física, mediante cualquier medio tecnológico, con la intención de dañar a su legítimo titular. Circunstancias agravantes especiales: que se utilicen las credenciales para vinculase a terceras personas, la concurrencia de extorsión hacia la victima o terceras personas.

2. https://www.linkedin.com/posts/cervierimonsuarez_noticiasuy-ugcPost-7233870571522932736-vV9d?utm_source=share&utm_medium=member_desktop

Con estos nuevos delitos, se busca dejar de encuadrar al Phishing dentro del delito de Estafa, contando ahora con normativa específica que contempla los nuevos actos ilícitos que se propagan por medios informáticos.

Recomendaciones para evitar el Phishing

A fin de evitar ser suplantado dentro de internet o bien contar con los elementos necesarios para poder afrontar un caso de Phishing se recomiendan las siguientes acciones:

1. Respetar la imagen corporativa en los diseños y comunicación a fin de que los usuarios y consumidores no confundan fácilmente a la empresa con publicaciones de terceros.
2. Tener la marca registrada es recomendable puesto que las denuncias en internet se agilizan cuando se adjuntan documentos de respaldo de propiedad intelectual.
3. Mantener informados a los usuarios y consumidores del tipo de campañas publicitarias que se realizan y cuales no son propias de la empresa a fin de prevenir futuras estafas de Phishing.

por:

Dra.
Lucía Cantera

Asociada Senior
lcantera@cmlawyers.com.uy

Dra.
Isabel Méndez

Abogada
imendez@cmlawyers.com.uy

Dr.
David Oliva

Abogado Senior
doliva@cmlawyers.com.bo