Estafas y fraude: Consejos básicos para detectarlo

CIUDAD DE MÉXICO. 08 de noviembre de 2022.- La seguridad es un aspecto fundamental que deben cuidar todos los usuarios cuando navegan en línea. Sobre todo en fin de año, en donde el alto tráfico en los comercios *online,* por los descuentos de la temporada y el pago de aguinaldos, se convierten en un blanco muy atractivo para los ciberdelincuentes.

Pero el riesgo de fraude es latente durante todo el año. De hecho, la Condusef señala que tan solo en el primer semestre de 2022 se registraron 3.5 millones de reclamaciones por posibles fraudes en México, de los cuales el 59% corresponden a fraude cibernético.

Por lo anterior, las empresas deben seguir los siguientes pasos para detectar y protegerse de la incidencia de fraude electrónico, antes de tener un impacto negativo muy alto y afectar su reputación:

1. Ingeniería social, la clave

Se trata de una técnica que utilizan los ciberdelincuentes para ingresar a los sistemas de las empresas luego de ganarse la confianza de un usuario interno, al cual le pueden hacer caer en un engaño, enviar un *link* malicioso, y conseguir la ejecución de un programa con *malware*.

Es por eso que el primer consejo radica en la capacitación del personal de las empresas con respecto a las principales amenazas cibernéticas y cómo afrontar un acontecimiento sospechoso, sobre todo en materia de correos electrónicos maliciosos, mensajes de texto, ransomware y ataques DDoS (ataques de denegación de servicios)

2. Verifica tus plataformas

Esto se debe a que uno de los principales métodos para estafar a los usuarios es el robo de identidad. De hecho la Condusef señala que México es el octavo lugar en este delito a nivel global.

Este tipo de suplantaciones están presentes en distintos tipos de plataformas, incluso en las redes sociales y plataformas de empleos. Strike encontró una estafa sofisticada en LinkedIn en la que un usuario apócrifo ofrecía una oportunidad de inversión para *startups*, de la mano de supuestos inversores globales ubicados en Reino Unido.

Para generar confianza hacia los usuarios las empresas requieren de cuentas con un *check* verificado y URLs que tengan el protocolo de seguridad https://.

3. Evita las contraseñas

Hoy en día, según datos de North Pass, aún existen 103.170.552 de usuarios cuya contraseña puede ser descifrada en tan solo 1 segundo.

Por ello, es importante que las marcas ofrezcan plataformas en las que puedan comprar o transaccionar utilizando sus datos biométricos, que son aquellos datos que surgen de la medición y cómputo de las características humanas de cada persona, como las huellas dactilares, el reconocimiento facial y la voz.

4. 'Hackea' tus propios sistemas

De inmediato cualquier encargado de TI sin conocimientos sobre el *hacking* ético, diría que no. Pero una de las soluciones más eficientes en la actualidad es el *pentesting*, una técnica que radica en contratar a un experto en ciberseguridad para entrar a su sistema y encontrar posibles vulnerabilidades que un *hacker* podría aprovechar para realizar un ataque.

El Striker, que es el encargado de hacer este proceso, es un *hacker* ético experto en ciberseguridad que usa sus habilidades de *hacking* para el bien común. De ese modo, se adentra al sistema de una empresa pero no para obtener dinero o información privada, sino para ayudarle a protegerse.

De ese modo, las empresas se anticipan a los movimientos de los entes fraudulentos, protegen a sus sistemas y detectan cuáles son las 'puertas de entrada' que puede utilizar los cibercriminales y las 'cierran' antes de que éstos las encuentren.

El fraude cibernético es una amenaza latente que afecta a todo tipo de empresas, de diversos sectores y tamaños, durante todo el año. Si bien existen medidas para protegerse y mitigar el riesgo, las medidas como el *pentesting* deben ser recurrentes y nunca deben dejarse en el olvido ya que el cibercrimen nunca descansa. Por el contrario, cada vez se vuelve más sofisticado y evoluciona para seguir intentando perpetrar en los sistemas de las empresas en busca de 'vaciar sus arcas'.

Sobre Strike

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como "Strikers", una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: https://strike.sh/

Síguenos en nuestras redes sociales:

Instagram - @strikesecurity
Twitter - @strike_secure
LinkedIn - Strike

Contacto para prensa México
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co

Contacto para prensa Colombia
another
Carla Hernández Alarcón | Sr. PR Expert
+57 3157200316
@carla.hernandez@another.co