Vishing: la ‘nueva voz’ de los ciberdelincuentes de la que debes cuidarte

CIUDAD DE MÉXICO. 08 de septiembre de 2020.- ¿Has recibido llamadas a nombre de un banco o una empresa indicando que hay cargos no reconocidos o fallas en tu servicio? Cuidado. Durante los últimos meses, el incremento del trabajo -remoto derivado del confinamiento por el COVID-19- ha motivado a los ciberdelincuentes a migrar a una modalidad que, si bien no es nueva, ha cobrado popularidad: el *vishing*.

Su nombre proviene de la combinación de las palabras ‘*voice*’ y *‘phishing’* y se trata de estafas por teléfono. La finalidad de este ataque es robar los datos de las personas para obtener un beneficio económico.

Para los ciberdelincuentes se ha vuelto muy sencillo atacar de este modo. Más allá del número telefónico, los criminales no necesitan conocer más detalles o datos como la dirección de la víctima y ni siquiera su nombre para ejecutar la estafa. El *vishing* funciona mediante comandos de voz que, al contestar, le indican al usuario que existe alguna falla en alguno de sus servicios o que existen movimientos no reconocidos dentro de una cuenta bancaria, por mencionar ejemplos. Para conocer más detalles, indica la grabación, el usuario debe presionar la tecla “1”. Es ahí en donde comienza la estafa, ya que la víctima es redirigida con un interlocutor humano, quien le explica a detalle el falso inconveniente y le pregunta datos bancarios y de carácter personal, con el supuesto fin de autenticar las información del cliente.

Los atacantes eligen un servicio legítimo y popular como una institución bancaria, sistemas de telefonía, televisión por cable o tiendas de autoservicio, entre otros. Esto hace que las víctimas, al notar que la llamada supuestamente proviene de una marca o empresa legítima, sientan confianza de compartir información con la persona del otro lado del teléfono.

Aproximadamente 60 palabras o 30 segundos al teléfono suelen ser suficientes para crear una interacción exitosa con la víctima. En Reino Unido se presentaron diversos casos de este tipo a nombre de Amazon. Las personas recibían el mensaje de una voz, muy similar a la de Siri, con un guión corto y claro:

“Su pedido de Amazon por (cualquier cantidad) de libras esterlinas fue enviado. Recibirá este paquete en los próximos días”, indica el mensaje. *“Para cancelar el pedido o conocer más detalles, presione 1”,* añade.

Personal de Sophos recibió la llamada y presionó 1 a modo de experimento (no recomendamos hacerlo en caso de recibir una llamada de este tipo). Luego de presionar la tecla 1 el usuario es redirigido a lo que parece ser un *call center* legítimo de la empresa. Es entonces donde se le

comienzan a hacer preguntas al usuario sobre su correo electrónico y contraseña de la cuenta de Amazon, datos bancarios y de sus métodos de pago frecuentes, entre otros, todo con el supuesto fin de autenticar su información de cliente.

¿Por qué funcionan este tipo de ataques?

Las víctimas suelen caer ya que, por lo general, las llamadas se reciben dentro de una red móvil o fija dentro del mismo país, por lo que el usuario ve un número local creíble y contesta. Actualmente, las llamadas de voz mediante grabadoras son ampliamente utilizadas por empresas legítimas, por lo que los usuarios no suelen sospechar. Los delincuentes que realizan estas llamadas solo tratan con personas que denominan 'Activas', es decir, aquellas que ya presionaron la tecla "1", lo que ahorra algunos pasos en la estafa, contrario a tener que captar la atención de una una persona desde cero. Un último detalle es que los ciberdelincuentes cambian constantemente la línea telefónica que utilizan, por lo que guardar estos números en la lista de contactos bloqueados no ayudará mucho si se quiere evitar ser contactado.

¿Qué hacer al respecto?

Es difícil detectar y distinguir entre una llamada legítima y una fraudulenta de este tipo, pero la recomendación más común es no compartir datos sensibles, como información bancaria y datos personales, con ninguna empresa ya sea por teléfono o correo electrónico.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) recomienda no responder llamadas o mensajes de remitentes desconocidos y tomar en cuenta que las entidades bancarias y compañías advierten, de forma recurrente, que nunca solicitarán datos de este carácter mediante este tipo de canales. También señala que, ante cualquier inconveniente, debe ser el usuario el que llame directamente a la institución en cuestión y no al revés, además de que en ningún caso se debe proporcionar información financiera a desconocidos.

###

Sophos, incluida la solución de endpoint Intercept X y el firewall de próxima generación XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/