VISHING y la Inteligencia Artificial como herramienta de ataque

CISO Global LATAM

CISO Global LATAM

10.182 seguidores

Seguir

24 de julio de 2023

Abrir lector interactivo

Durante los últimos años se han hecho comunes en Internet testimonios que denuncian estafas a través de llamadas en las cuales, quienes se encuentran del otro lado del teléfono, suplantan la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal de sus víctimas. Es esto, precisamente, lo que se denomina Vishing.

Según explica David Alfaro, General Manager de CISO GLOBAL para Latam, “quienes utilizan el Vishing llaman por teléfono y se hacen pasar, por ejemplo, por un ejecutivo del banco o un familiar. Una vez que tienen la confianza de su interlocutor intentan sacarle información personal, para así acceder a sus cuentas bancarias, redes sociales o recopilar datos que les puedan ser útiles para un ataque”.

“La nueva tendencia —agrega— es apoyarse en herramientas de Inteligencia Artificial para clonar la voz de una persona conocida con fines fraudulento. De esta manera, la víctima es mucho más propensa a creer que efectivamente está hablando con alguien a quien conoce”.

¿Cómo protegerse del Vishing?

Alfaro señala que en una de las estafas más comunes la persona que llama se hace pasar por empresas muy conocidas y —tras señalar que la computadora de la víctima se encuentra infectada— pide acceso remoto al sistema. En los pocos casos que tengan éxito, accederán a una serie de datos privados. Esto también aplica a robos de cuentas de Chats solicitando el código de recuperación de la cuenta recibido por SMS.

Para una protección adecuada frente al Vishing, el ejecutivo entrega las siguientes recomendaciones:

· No confíes en el identificador de llamadas: Quienes se dedican a este tipo de estafa a menudo falsifican el número, por lo que puede parecer que proviene de una organización legítima.

· Cuidado con los links: Nunca descargue softwares o pinches un link a pedido de una persona que llama.

· No entregar información: Nunca entregues a la otra parte información que ya debería tener. Un ejemplo: si te llaman desde el banco, no deberían pedirte tu número de cuenta. Deberían saberla. Tampoco datos de tu cuenta o tarjetas de coordenadas.

· Desconfía: Cada vez que alguien te llame y cree una tremenda sensación de urgencia o presión, desconfía mucho. Están tratando de apresurarte a cometer un error. Incluso si la llamada telefónica parece estar bien al principio, si comienza a sentirse extraña, puede detenerse y decir "no" en cualquier momento.

· Llama a la persona conocida: En caso de que sospeches de la llamada de una persona conocida, la forma más simple de identificar si es una estafa, es colgar y llamar directamente a la persona para confirmar su identidad.

· No des nombres ni preguntes por nombres: Evita preguntar si quien llama es tal o cual persona, pues ese dato será tomado y usado.

Desde CISO Global LATAM creemos que una sólida cultura de Ciberseguridad y Resiliencia garantizan la continuidad de tu negocio ante este tipo de ataques que cada día se profesionaliza más.