Publicado en Madrid el 19/10/2020

S2 Grupo establece las 5 claves básicas para protegerse de los ataques de "vishing"

Ante el incremento de casos de ciberdelitos tipo "vishing" en los últimos meses, expertos de la empresa española S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, han establecido cinco claves que nos ayudarán a protegernos y evitar caer en las redes de ciberdelincuencia

El vishing consiste en llevar a cabo estafas a través de llamadas telefónicas con el fin de robar dinero. Su nombre se debe a la similitud con el ya conocido “phishing”, un engaño en el que se suplanta la identidad de una persona u organización para robar dinero, datos o para inyectar código malicioso en los equipos de las víctimas.

En el caso del vishing, las realizan ciberdelincuentes que quieren ganarse la confianza del interlocutor haciéndole creer que son operarios de alguna compañía o entidad de relevancia, como la compañía telefónica o la Seguridad Social, por ejemplo. En este sentido y para dar mayor credibilidad a sus mensajes, dan datos personales a sus víctimas (número de contacto, ubicaciones, etc) que obtienen en Redes Sociales y webs de intercambio o compraventa, como Milanancios o Wallapop. Entonces, a través de diferentes mecanismos, consiguen obtener dinero de estas personas de forma ilícita.

Desde S2 Grupo, se ha destacado que otras formas habituales de conseguir dinero a través de los ataques tipo vishing es hacerse pasar por compañías telefónicas para acabar haciendo que sus víctimas les hagna un ingreso por medio de aplicaciones de pago online. También pueden fingir ser técnicos de Microsoft para alertar de un problema e instalar programas espía en el ordenador que roba las credenciales bancarias. Otras de las técnicas más usadas por los delicnuentes consiste en que hacen que sus víctimas llamen a teléfonos de tarificación muy elevada o hacen creer que llaman de la compañía de suministro eléctrico, alertando de que deben pagar inmediatamente el pago de las últimas facturas o si no se corta el servicio en ese momento.

“Con la crisis del Covid hay más familias con situaciones económicas realmente complicadas y esta vulnerabilidad está siendo aprovechada por los atacantes. Este verano, por ejemplo, se destapó el vishing relacionado con la Seguridad Social en el que hacían creer que iban a hacer una devolución de 300 euros por Bizum para que llegara lo antes posible y el interlocutor en lugar de cobrar, lo que hacía en realidad era pagar esa cantidad”, ha explicado José Rosell, socio-director de S2 Grupo.

“El delincuente al colgar, lo que hacía era enviar una solicitud de cobro a esa persona en lugar de solicitud de pago. Esto generaba confusión y unido a la inexperiencia de muchos usuarios con el sistema o por simple precipitación, aceptaban ese cobro, sin darse cuenta de que realmente lo que hacían era pagar y no cobrar. Para evitar estas situaciones, es muy importante evitar actuar con rapidez y, si tenemos alguna duda, consultar con alguna persona de confianza antes de realizar alguna acción”, ha detallado Miguel A. Juan, socio-director de S2 Grupo.

Cinco consejos de lo que se debe y no se debe hacer

Ante esta situación que ha ido incrementándose exponencialmente desde el verano, expertos de S2 Grupo han destacado cinco claves que ayudarán a prevenir caer en las redes del vishing:

Nunca facilitar datos sensibles como cuentas bancarias, números de tarjeta de crédito ni de seguridad como la fecha de caducidad o el código de seguridad de tres números.
Si se recibe una llamada que haga dudar, colgar y buscar la manera de contactar de nuevo con la supuesta compañía que ha llamado. Si es una compañía oficial se podrá hacer sin problema.
Desconfiar de llamadas realizadas a través de números ocultos.
Instalar algún tipo de aplicación de llamada que alerte ante un posible caso de fraude por los filtros anti-spam que incorporan.
Alertar de estos timos a las personas más vulnerables, como suelen ser los mayores, porque suelen ser más susceptibles a las estafas.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Ciberseguridad Dispositivos móviles