GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

GUARDIA CIVIL
DIRECCION ADJUNTA OPERATIVA
ZONA DE MADRID
COMANDANCIA DE MADRID

FDI 01/2024

FICHA DE DIFUSIÓN DE INFORMACION

ESTAFA DENOMINADA “VISHING”

COOPERA SP

Tres Cantos, 08 de enero de 2024

La estafa del “VISHING”

- **¿En qué consiste?**

En el último año se ha detectado en demarcación de la Comandancia de Madrid un aumento significativo del número de víctimas que se habrían visto perjudicadas por una modalidad de ciberestafa conocida como “***Vishing***”.

El Vishing es un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

La presente ficha tiene por objeto informar y sensibilizar sobre esta modalidad de ciberestafa, dando recomendaciones para prevenir ser víctima de esta modalidad delictiva.

- **Modus operandi**

- Los ciberestafadores realizan llamadas telefónicas haciéndose pasar por entidades bancarias, empresas de mensajería o un servicio para obtener información privada de las personas o para conseguir que instalen un programa malicioso en sus equipos informáticos o teléfonos móviles.

- Previamente, buscan en internet y en redes sociales información básica de las personas a las que se van a dirigir para conseguir que la llamada parezca legítima.

- Con tales excusas, solicitan a su víctima el código para firmar operaciones que va a recibir normalmente mediante SMS.

PRINCIPALES TIPOS DE LLAMADAS DE VISHING

- **Engaño por premios/sorteos**: se informa a la víctima que ha ganado un premio o sorteo y le solicitan información personal para procesar su pago o gestionar los trámites.
- **Amenazas de cierre de cuenta**: Asegurar que la cuenta de la persona será cerrada o suspendida si no proporciona la información que se les indica.
- **Llamadas de soporte técnico falsas**: simulan ser personal del soporte técnico de una empresa conocida e indican que han de resolver incidencias.
- **Engaño por problemas financieros**: afirman que existen problemas relacionados con la cuenta bancaria de la persona y solicitan información personal o financiera para solucionar dicho problema.
- **Falsos mensajes de voz automatizados**: envían mensajes de voz automatizados a la persona solicitándoles información o que siga unas pautas.
- **Inversiones en criptomonedas o cuentas de ahorro**: realizan llamadas ofreciendo inversiones, garantizando importantes ganancias.

CARACTERÍSTICAS DE LAS LLAMADAS

- **Creación de urgencia**: afirman que la gravedad de los problemas aconseja actuar de inmediato, a fin de que la víctima no pueda realizar comprobaciones.
- **Solicitud de información confidencial**: buscan obtener información privada como números de tarjetas de crédito, contraseñas u otra información personal durante la llamada.
- **Amenazas o consecuencias**: realizan presiones firmes relacionadas con bloqueo de cuentas o sanciones
- **Instalación de programas**: convencen a la víctima de la necesidad de instalar un programa o aplicación en sus dispositivos para solucionar un problema.
- **Evitan preguntas**: no responden a preguntas sobre su identidad o legitimidad de la llamada.
- **Ofertas tentadoras**: ofrecen grandes beneficios para motivar a la víctima.

Recomendaciones.

- ***Verificar la identidad del llamante**. Si nos aparece un número desconocido en la pantalla de nuestro teléfono, una alerta de spam o no nos convence, comprobar el número de teléfono en Google para ver si está relacionado con algún tipo de fraude.*
- ***Desconfiar de aquellas llamadas que denoten un cierto grado de Urgencia**. Los ciberestafadores suelen trasmitir que hay problemas o se ha identificado actividad sospechosa para que la víctima actúe rápidamente sin pensar con claridad.*
- ***Si te ofrecen promociones demasiado ventajosas, desconfía**. Los ciberestafadores intentan captar tu atención anunciándote premios o propuestas seductoras, para que facilites datos por miedo a perder la oportunidad.*
- ***Cuando recibas una llamada sospechosa de fraude, no realices ninguna acción**. Contacta tú directamente con la entidad bancaria, buscando el número de teléfono en su página web oficial. No devolver nunca la llamada.*
- ***No facilitar claves de acceso o códigos de un solo uso (OTP)**. Las entidades bancarias no te llamarán para solicitarle información confidencial.*
- ***Bloquea los números de teléfono fraudulentos.** De esta manera conseguirás, que no se vuelvan a poner en contacto contigo.*

Tres Cantos, 08 de enero de 2024

PLAN COOPERA

GUARDIA CIVIL

WWW.GUARDIACIVIL.ES

COMANDANCIA DE LA GUARDIA CIVIL DE MADRID
DIRECCIÓN: C/ SECTOR ESCULTORES, 10 - TRES CANTOS (MADRID)
TELÉFONO: 91 807 39 00 - EXT. 44712
MADRID-SEGPRIVA@GUARDIACIVIL.ORG