CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA EVITAR UN ATAQUE SPOOFING

Los ataques a las conexiones inalámbricas son muy comunes, y los ciberdelincuentes se sirven de diversos software y herramientas para saltarse las medidas de seguridad, infectar o tomar control de nuestros dispositivos. Generalmente, este tipo de ataques se basan en interponerse en el intercambio de información entre nosotros y el servicio web, para monitorizar y robar datos personales, bancarios, contraseñas, etc., es importante conocer las formas en las que operan los atacantes. ¿Has escuchado el término spoofing? A continuación, te explicamos en qué consiste.

¿Qué es el SPOOFING?

1.- Es una técnica utilizada por los ciberdelincuentes para suplantar una identidad electrónica y así hacerse pasar por una empresa u otra persona, con el objetivo de cometer algún tipo de estafa.

Es un acto fraudulento en el que la comunicación desde una fuente desconocida se disfraza de fuente conocida.

¿Qué es el SPOOFING?

2.- Este ataque ocurre cuando una persona pretende ser otra, con el fin de inducir "a su víctima" a que comparta sus datos personales o haga alguna acción en nombre del falsificador.

Normalmente, el timador se esforzará en establecer una relación de confianza con su objetivo, para asegurarse de que comparta sus datos sensibles con más facilidad.

Tipos de SPOOFING:

- Spoofing de correo electrónico: Consiste en suplantar la dirección de correo de una persona o entidad de confianza, ejemplo el Phishing
- Spoofing de llamadas: Falsificación de un número de teléfono para hacerse pasar por una entidad de confianza.
- Spoofing de suplantación de página web: Es la creación de un sitio web idéntico en diseño y, en ocasiones con una URL similar, a una institución real.

Objetivos del SPOOFING:

- Obtener información confidencial de las víctimas, sirviéndose de la confianza que transmita la identidad suplantada.
- Robar credenciales, datos bancarios como los números de nuestras tarjetas bancarias.
- Engañarnos para que ejecutemos o descarguemos algún malware en nuestros computadores o dispositivos móviles.

¿Cómo PROTEGERSE?

1.- Llama en caso de duda. Si recibes un correo pidiéndote información personal, contraseñas o solicitan dinero, llama al remitente si lo conoces. De lo contrario, ignora el mensaje.

2.- Ingresa tú la URL. Asegúrate que el sitio web al que ingresas es el oficial. Si dudas de un enlace, mejor busca directamente el sitio.

¿Cómo PROTEGERSE?

3.- Nunca descargues archivos adjuntos, aunque provengan supuestamente de una entidad conocida (SII, PDI, Fiscalía, Tesorería y Bancos), sobre todo si no lo estás esperando.

4.- Sé escéptico. Si te piden datos personales, duda y no entregues tu Rut, contraseñas, coordenadas bancarias, etc.

CURIOSIDADES:

Sabías que uno de los casos más famosos de spoofing es el del juego para dispositivos móviles Pokémon GO, el cual permitía a los entrenadores cambiar su ubicación a través del GPS para así recoger criaturas sin moverse de su propia casa.

Si recibes correos falsos o detectan algún sitio fraudulento

DENUNCIA AL **CSIRT** 24/7

(+562) 2486 3850

También puedes denunciar a la **PDI**

(+562) 2708 0658