CONCIENCIACIÓN EN CIBERSEGURIDAD

Protegiendo tus datos

CONTENIDO DE LA PRESENTACIÓN

ÍNDICE

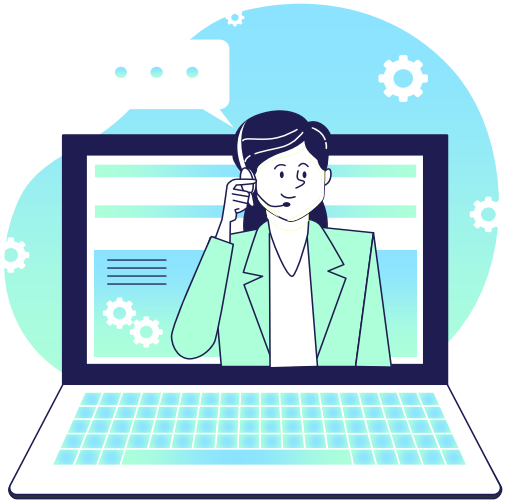
INTRODUCCIÓN

La ciberseguridad es responsabilidad de todos.

Hoy hablaremos de Pretexting/Vishing, Smishing y los riesgos de las redes sociales.

01 PRETEXTING VISHING

PRETEXTING/VISHING



Pretexting/Vishing es una estafa en la que los estafadores se hacen pasar por personas de confianza para obtener información confidencial por teléfono.

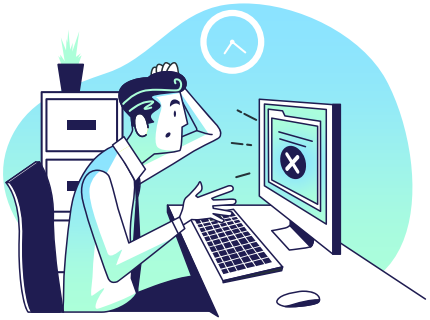
¿Cómo podemos evitarlo?

- Verificando la identidad de quien llama.
- No compartiendo información confidencial por teléfono sin confirmar.

¿Cómo identificarlo?

- Llamadas inesperadas pidiendo datos sensibles.
- Falsos pretextos para obtener información personal.

PROBLEMA VS. SOLUCIÓN (PRETEXTING/VISHING)



Problema

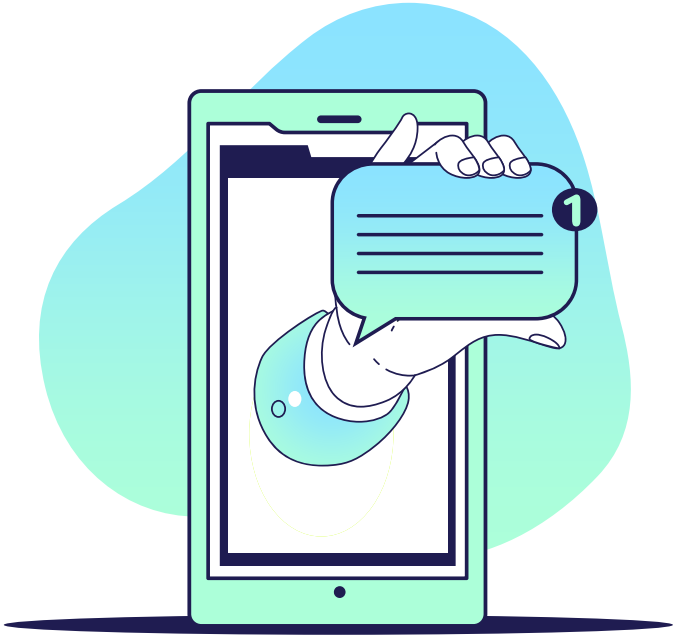
Recibes una llamada de alguien que dice ser tu banco, solicitando información personal y financiera para “verificar” tu cuenta.

Solución

En lugar de proporcionar información de inmediato, cuelga y busca el número oficial de tu banco en su sitio web o en una fuente de confianza.

02
SMISHING

SMISHING



Smishing es una estafa en la que los atacantes utilizan mensajes de texto para engañar a las personas. Suelen contener enlaces maliciosos o solicitudes falsas que buscan robar información.

¿Cómo podemos evitarlo?

- No haciendo clic en enlaces de mensaje de texto de remitentes desconocidos o sospechosos.
- Desconfiar de mensajes de texto que solicitan información personal o financiera.
- Si recibes un mensaje sospechoso, comunícate directamente con la empresa o entidad involucrada a través de sus canales oficiales para verificar la autenticidad de la solicitud.

EJEMPLOS DE MENSAJES SMISHING.

EJEMPLO 1

Has ganado un premio y necesitas hacer clic en un enlace.

EJEMPLO 2

Una notificación con supuestas deudas pendientes.

EJEMPLO 3

Problemas en tu cuenta bancaria con un enlace para “solucionarlos”.

EJEMPLO 4

Ofertas de productos o servicios demasiado buenas para ser verdad, solicitando un clic para comprar.

EJEMPLO 5

Supuestos problemas con entregas de paquetes o enviós de servicios de mensajería.

EJEMPLO 6

Has sido inscrito en un servicio de suscripción costoso y debes hacer clic para cancelarlo.

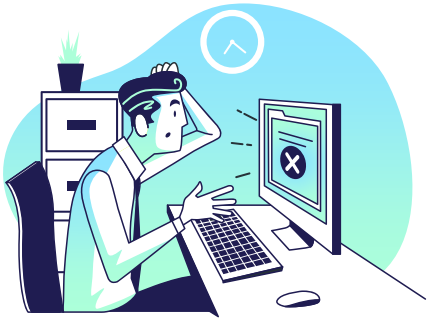
03
REDES SOCIALES

REDES SOCIALES

A pesar de su utilidad, las redes sociales conllevan **riesgos**, como la **exposición de información personal** y la interacción con desconocidos.

En la siguiente sección, exploraremos cómo podemos navegar por las redes sociales de **manera segura** y consciente, protegiendo nuestra información personal, reconociendo las amenazas y manteniendo un entorno en línea seguro.

RIESGOS Y PROTECCIÓN EN REDES SOCIALES



RIESGOS

- Exposición de datos personales.
- Interacción con desconocidos.
- Contenido malicioso.

PROTECCIÓN

- Limita la información personal.
- Verifica identidades antes de conectar.
- Evita abrir enlaces y archivos sospechosos

04
CONSEJOS GENERALES

CONSEJOS GENERALES DE CIBERSEGURIDAD

- Utiliza contraseñas fuertes y únicas.
- Actualiza regularmente tu software y aplicaciones para corregir vulnerabilidades.
- Protege tus dispositivos con software antivirus o cortafuegos.
- Sé cauteloso con los correos electrónicos y enlaces sospechosos.
- Mantén una copia de seguridad de tus datos importantes.