Cuidado con el

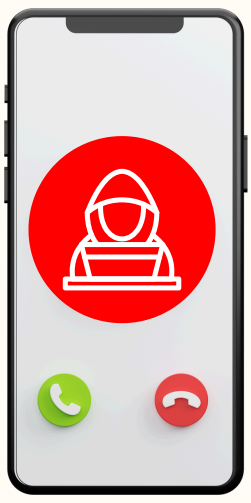
Ciberataque de 2 pasos

El vishing o “phishing de voz” se produce cuando un ciberdelincuente intenta convencerte de que facilites información delicada por teléfono.

¿Cómo funciona?

Paso 1

El estafador se presenta como un representante de una empresa legítima, alegando un problema urgente como fraude o cambios en los servicios, y solicita información de tus cuentas para **"ayudarte".**



Paso 2

Una vez que logran ganarse tu confianza, solicitan información sensible como números de cuenta, códigos de seguridad o que realices una transferencia a una cuenta que parece "segura".

Y eso es todo; con esta información, tendrán la capacidad de acceder a tus cuentas y utilizarlas de manera indebida.

Así que antes de proporcionar tus datos, checa estas red flags...

- Los estafadores crean urgencia con problemas como fraude o servicios suspendidos para apresurar decisiones.
- Se solicitan datos personales o financieros, como contraseñas y números de tarjeta de crédito, bajo la excusa de "verificación".
- Buscan atraerte con ofertas irresistibles o premios sorpresivos que requieren la entrega de datos personales.

⚠️ ⚠️ ⚠️

Si detectas alguna de estas señales, finaliza la llamada y verifica directamente con la institución que supuestamente se comunicó contigo.

¡No caigas en la trampa!

TU LOGO AQUÍ

Grupo Smartekh | Security Culture Management