Ciberseguridad: una misión compartida

INGENIERÍA SOCIAL, *EL ARTE DEL ENGAÑO*

La ingeniería social consiste en engañar a la víctima para que revele, voluntariamente, información sensible o haga acciones que vulneren la seguridad de los datos y dispositivos que maneja.

Tipos de fraudes online más habituales

Phishing

Smishing

Vishing

Sextortion

Baiting

Brushing

Dumpster diving

Shoulder surfing

Seis consejos para identificar estos fraudes:

1. Verificar siempre el remitente de los correos electrónicos (Phishing). Los atacantes suelen utilizar direcciones que se parecen mucho a las reales, pero con pequeñas variaciones.

2. Presta máxima atención a las **llamadas de teléfono fraudulentas (Vishing) y los SMS engañosos (Smishing)** que se sirven de la sensación de urgencia, curiosidad o miedo para manipular al destinatario y que éste realice una acción no deseada.

3. Compartir contraseñas mediante métodos no cifrados supone poner en riesgo las cuentas, así como la información que contienen. Ningún sector (banca, telefonía, sanidad...) pedirá tus contraseñas por teléfono, chat o similar.

4. Proteger los datos personales de nuestros ciudadanos. Manejamos información sensible, así que evita revelar información personal de terceros ante peticiones extrañas por teléfono o correo electrónico sin antes verificar la identidad del remitente.

5. La formación y concienciación en ciberseguridad es fundamental para que los usuarios estén prevenidos y sepan cómo actuar ante posibles riesgos cibernéticos en el ámbito laboral y personal, por ello en las entidades públicas es necesario promover estas acciones para garantizar la seguridad de la información de la organización.

6. Reportar cualquier comportamiento anómalo a tu soporte de Ciberseguridad o de Tecnologías de la Información.

GENERALITAT VALENCIANA
Conselleria d'Hisenda, Economia i Administració Pública

CSIRT-CV
Centro Seguridad TIC de la Comunitat Valenciano

www.csirtcv.gva.es
concienciat.gva.es