TIC INFORMA

TÉCNICAS DE INGENIERÍA SOCIAL: ¿CÓMO CONSIGUEN ENGAÑARNOS?

Existen una serie de acciones y técnicas de ingeniería social, desarrolladas por ciberdelincuentes, que debemos conocer. Por ello, en esta entrega, el Departamento de Tecnologías de la Información y Comunicaciones (TIC) informa a la Comunidad Minsal las características de estos métodos, para así estar más atentos e impedir nuestra -involuntaria- colaboración.

HISTORIA FICTICIA

Base de cualquier ataque de ingeniería social

Consiste en elaborar un escenario/historia ficticia, donde el atacante tratará que la víctima comparta información que, en circunstancias normales, no revelaría (Pretexting).

PRESIÓN INDEBIDA

Chantaje donde se busca amenazar a la víctima

En este caso, se amenaza con distribuir contenido supuestamente comprometido a contactos (aunque no exista tal contenido), si no se accede a las peticiones del ciberdelincuente, generalmente a realizar un pago.

PHISHING

Busca "pescar" víctimas

Generalmente se emplean correos electrónicos con archivos adjuntos infectados o links a páginas fraudulentas, con el objetivo de tomar el control de los equipos y robar información confidencial.

SMISHING

Se trata de una variante del "phishing" pero que se difunde a través de SMS

Se pide al usuario que llame a un número telefónico o que acceda a un enlace de una web falsa.

LLAMADAS TELEFÓNICAS (VISHING)

Llamados falsos, historias falsas

En esta técnica, el atacante se hace pasar por una organización/persona de confianza, para que la víctima revele información privada.

REDES SOCIALES

Atención a cupones de descuento y juegos

Las técnicas de engaño más comunes a través de las redes sociales son mediante cupones de descuento, juegos y concursos, donde crees que puedes ganar algo.

MIRAR ENCIMA DEL HOMBRO

También conocido como "Shoulder Surfing"

Al atacante le basta con observar lo que escribe o tiene en pantalla otro usuario (para obtener información muy útil).

CORREOS DE REMITENTES FALSOS

Suplantan la identidad de una organización, mediante un correo de remitente falso.

Pueden enviar correos phishing para robar claves de acceso bancarias, así como difundir malware, o robar información de la organización, en busca de un beneficio ilícito.

SUPLANTACIÓN DE PROVEEDORES, AUTORIDADES U OTROS FUNCIONARIOS

El ciberdelincuente suplanta a un proveedor o autoridad, con el objetivo de obtener información confidencial, datos bancarios y claves de acceso.

Suelen utilizar correos y páginas web muy parecidas al legítimo. Asimismo, se pueden contactar telefónicamente, indicando que es urgente el envío de la información, sin dar tiempo para pensar o corroborar.

Bienvenidas las consultas a seguridadtic@minsal.cl