ZURICH

Ingeniería Social ataca el eslabón más débil de la Ciberseguridad

¿QUÉ ES LA INGENIERÍA SOCIAL?

La Ingeniería social consiste en manipular a una persona a través de técnicas psicológicas y habilidades sociales de manera de conseguir información de su interés y/o ganar acceso a los sistemas. Dependiendo de la influencia que tenga el ciberdelincuente será el resultado obtenido con o sin utilización de la misma tecnología.

¿EL USUARIO ES EL ESLABÓN DÉBIL DE LA CIBERSEGURIDAD FRENTE A LA INGENIERÍA SOCIAL?

Definitivamente, sí. Varios estudios indican que el factor humano es la vulnerabilidad latente de Ciberseguridad. Todo radica en la forma de ser de las personas. Pensemos que: “En la mayoría de las situaciones queremos ayudar”, “Es difícil para algunos decir que NO”, “Tratamos de ser empáticos, entregando confianza”. Y estos aspectos aumentan la posibilidad para el ciberdelincuente explotar dicha vulnerabilidad.

¿CÓMO SE CONFIGURA LA INGENIERÍA SOCIAL?

El Ciberdelincuente actúa bajo las siguientes fases:

- Recolección de información, trata de obtener información sobre la víctima para ir creando un escenario de ataque.
- Relación de confianza, preparado el escenario comienza a atraer a la víctima y establecer un buen nivel de confianza.
- Manipulación, a esta altura se ejecuta el ataque buscando conseguir un determinado objetivo.
- Salida o corte, en este punto elimina la interacción con la víctima e intenta borrar las huellas de las comunicaciones.

¿QUÉ PUEDEN LOGRAR HACER CON LA INGENIERÍA SOCIAL?

La información que ellos obtienen, la podrán utilizar para la materialización de:

Generar que caigas en un Phishing enviado por correo electrónico.

Ingresar credenciales en páginas maliciosas o que termines enviando tus datos personales, por medio de SMS.

Recibir llamadas falsas y ejecutar acciones destinadas a la estafa o fraude y muchas más...

¿CÓMO EVITAR SER VÍCTIMAS DE ATAQUES DE INGENIERÍA SOCIAL?

- Concientización, es la palabra clave para conocer este tipo de ataque, el impacto que tiene y las técnicas que utilizan. De manera de reducir el porcentaje de víctimas.
- Ser cuidadoso con nuestra información, no debemos exponer los datos en foros abiertos o comentarios en páginas web.
- No abrir links ni adjuntos sospechosos, ya que cualquier escenario posible tratará de obtener que tú caigas en algún fraude o estafa.
- Restringir la confianza, dudar de lo solicitado o informado dándote el tiempo para contrastar lo que el ciberdelincuente te indique.
- Generar Política de contraseñas y 2FA, emplear una contraseña robusta, cambiarla cada cierto tiempo y usar el 2FA (Doble autenticación) para una capa extra de protección a nuestros dispositivos y servicios.
- Protección de Dispositivos, manteniendo actualizado el sistema operativo y el antivirus.
- Verificar la seguridad de las webs donde introducimos datos personales.

El Grupo Zurich, está comprometido con la Seguridad de la información y es por ello, que extendemos la conciencia y la Cultura Ciber hasta tu hogar.

Recuerda: “Que las técnicas de Ingeniería social utilizadas para generar ciberdelitos se han valido incluso del hackeo emocional de los usuarios. Es por ello, que debes estar preparado y alerta”

#NO ME QUEDO OFF LINE