INGENIERÍA SOCIAL

Ingeniería Social

Independientemente de la magnitud de un ataque cibernético, la ingeniería social tiene un papel protagónico en su ejecución.

La **ingeniería social** tiene sus bases en la manipulación psicológica, es decir, lograr que las demás personas realicen cosas que otra persona desea que ejecuten.

Por ejemplo, obtener permiso para llegar tarde al trabajo o a la casa, por medio de la adulación; o lograr que el profesor modifique una calificación, a través de chantaje sentimental.

En el ámbito del crimen cibernético se define como un método utilizado por los delincuentes, para obtener acceso ilegítimo a la información de sus víctimas.

Existen cinco aspectos que se identifican en la ingeniería social:

- Puede ser de forma física o digital.
- Su calidad puede variar.
- También es utilizada por los gobiernos de los países.
- Puede pasar desapercibida fácilmente.
- Su enfoque es principalmente en las empresas.

Tipos de ataques

Phising
Recibes un correo electrónico de una empresa o entidad reconocida y te solicita que ingreses a cierta liga o envíes información confidencial como contraseñas o números de cuenta. La página puede ser una réplica exacta del sitio oficial.

Vishing
Realizan llamadas telefónicas suplantando la identidad de una persona o entidad para conseguir información de tipo confidencial.

Baiting
Hoy los criminales dejan dispositivos de almacenamiento, como memorias USB, infectados con malware para que los empleados curiosos las ingresen en los equipos y sean infectados.

Smishing
Por medio de mensajes de texto, se solicita que hagan clic sobre un enlace, descarguen un archivo o envíen información confidencial.

Scammer
Hoy utilizan los portales de citas online para conocer personas, principalmente solteros de edad avanzada, envían fotografías cada vez más sugerentes y posteriormente solicitan apoyo económico para realizar viajes y concertar una cita en persona.