La ingeniería social es un método para obtener información confidencial por medio de la manipulación de personas, logrando obtener la información a través de la víctima, sin tener que robarla por otros medios.
Esta técnica puede ser utilizada por investigadores, criminales o piratas informáticos.

Hablando de seguridad informática, un ingeniero social podrá utilizar cualquier herramienta tecnológica, como computadoras, teléfono, Internet, etcétera, para poder contactar a su víctima y obtener datos confidenciales, ya sea haciéndose pasar por algún agente de ventas, compañero de trabajo, soporte técnico, agente bancario, entre otros.

Pero el pirata informático también puede obtener la información cara a cara, haciéndose pasar por algún otro empleado de alto rango, empleando jerga técnica y política para obtener los datos de la víctima, como contraseñas, códigos, etcétera.

Para evitar esto, es común que las empresas entrenen a sus empleados para el uso de políticas de seguridad, para poder hacer que cualquier empleado o persona no sea vulnerable a la manipulación verbal de un ingeniero social.
Según Kevin Mitnick, la ingeniería social se basa en cuatro principios, que son:

1.- Todos queremos ayudar
2.- El primer movimiento es siempre de confianza hacia el otro
3.- No nos gusta decir No
4.- A todos nos gusta que nos alaben

La ingeniería social podría ser el método más fácil para cualquier delincuente cibernético, ya que se evita la molestia de buscar vulnerabilidades en los sis-temas o tener que empleado programas de “hacking” para obtener los datos confidenciales, ya sea por medio de keyloggers, troyanos o cualquier otro software especializado.

En América Latina es muy común que criminales utilicen la ingeniería social, no sólo para delitos informáticos, sino para extorsiones o secuestros, empleando la ingeniería social para hacerse pasar por familiares, agentes de aduana, técnicos de telefonía celular, etc.

Por esto es importante saber qué hacer cuando recibimos una llamada inesperada, de algún número privado o que simplemente no se conoce. La mejor opción para muchos es simplemente no responder, pero en caso de hacerlo, hay que escuchar a la persona, en caso de tratarse de un familiar en problemas, hay que escuchar cuidadosamente, no entrar en pánico, y nunca facilitar datos personales como nombre, apellidos, teléfonos, cuentas bancarias, etcétera, posteriormente, tratar de localizar al familiar y confirmar su paradero.

Regresando al tema informático, cuando alguna persona llama para “actualizar datos”, ya sean bancarios o de otra institución, se debe sospechar automáticamente, ya que por lo general ninguna empresa hace eso. Si en el proceso de la llamada, el supuesto agente solicita datos como nombres de usuario y contraseñas para verificar que esté llamando con el cliente correcto, es 99% seguro que se trate de un robo de identidad en proceso.
Ante esto, es recomendable tratar de obtener datos del mismo ingeniero social, como nombre y puesto, aunque seguramente dará información falsa, podría ayudar en futuras investigaciones. Seguido de investigar el número telefónico del que se recibió la llamada.