

LA INGENIERÍA SOCIAL

Es un término utilizado para un gran abanico de actividades maliciosas realizadas a través de las interacciones humanas. Utiliza la **manipulación psicológica** para -----, para que ----- de seguridad o faciliten -----; en pocas palabras, es el arte de manipular en su más pura esencia a las personas para que nos den lo que queremos, a lo que se le une la falta de conocimiento de las formas en las que estos pueden hackearnos.

Los ataques de ingeniería social se producen en uno o varios pasos: en primer lugar, **el agresor investiga a la víctima** para ----- necesaria como por dónde comunicarse con ésta y los protocolos que debe llevar a cabo el ataque; a continuación, **el atacante actúa** para ----- de la víctima y usa palabras adecuadas para que el usuario objetivo caiga y así romper la seguridad, ya que le revelará información sensible o concederá acceso a sitios.

Lo que hace que **la ingeniería social sea especialmente peligrosa** es que ----- más que en las vulnerabilidades del software o aplicaciones; por ejemplo, un atacante podría llamar a un usuario objetivo y fingir ser un miembro del personal de soporte para engañarlo y así que le dé su contraseña.

Como la ingeniería social tiene tanto éxito, los **ataques basados en el phishing y el robo de identidad** han aumentado un 500% en los últimos años. Según la Oficina Federal de Investigaciones, la ingeniería social cuesta las organizaciones 1600 millones de dólares en todo el mundo y pagan una media de 11,7 millones de dólares anuales por delitos de ciberseguridad.

Los ataques de ingeniería social pueden tener diferentes formas: por ejemplo, **de correo electrónico**, a través del cual, si un delincuente consigue hackear o aplicar ingeniería social a la ----- de una persona, tendrá acceso a éste y como la mayoría de la gente utiliza -----, probablemente también tenga acceso a las redes sociales de esta persona por ejemplo; por otro lado, los **ataques de phishing son un tipo muy usado** en esta estrategia de ingeniería social que ----- e inventan un escenario lógico para entregar las credenciales de acceso u otros datos personales.

También te pueden pedir que hagas una donación para su recaudación de fondos de caridad o alguna otra causa o **te presentan un problema** que necesitan que verifiques -----; incluso hay casos de **premios que has ganado** de ----- y que piden que reclames los delincuentes. También pueden fingir que responden a tu solicitud de ayuda, eligen empresas que utilizan millones de personas como una empresa de software o un banco: si no utilizas el producto o el servicio ignorarás el correo electrónico, la llamada telefónica o el mensaje pero si, por casualidad, lo usas, hay muchas posibilidades de que respondas porque probablemente sí quieras ayuda con un problema.

Como podéis ver **los ingenieros sociales manipulan los sentimientos humanos** como la ----- o el ----- para llevar a cabo sus planes y

hacer caer a las víctimas en sus trampas; por lo tanto ten en cuenta los siguientes consejos:

Primero - **No abras correos electrónicos ni archivos adjuntos** de ----- si no conoces el remitente en cuestión: no tienes por qué responder a un correo electrónico; incluso si lo conoces y sospechas de su mensaje, coteja y confírmalo. Las **ofertas extranjeras** son -----: si recibes un correo electrónico de una lotería o un sorteo extranjero, **dinero de un familiar desconocido o solicitudes de transferencia de fondos** de un país extranjero para obtener una parte del dinero, está garantizado que se trata de una -----.

Desconfía de las ofertas tentadoras - si una oferta suena demasiado succulenta piénsalo ----- antes de aceptarla: buscar en Google el tema puede ayudarte a determinar rápidamente si se trata de una oferta legítima o de una trampa.

Utiliza la autenticación multifactor - una de las informaciones más valiosas que buscan los atacantes son las credenciales de los usuarios: **el uso de la autenticación multifactor** ayuda a garantizar la ----- de tu cuenta en caso de que el sistema se vea comprometido ya que se necesitará algo más que solo tener tu contraseña.

Mantén actualizado tu software antivirus y asegúrate de que las actualizaciones automáticas están ----- o acostúmbrate a estar pendiente de ellas - **comprueba periódicamente** que se han aplicado las actualizaciones y **analiza tu sistema** en busca de posibles -----.

Al final, te ponemos un ejemplo fuera del mundo virtual - no importa cuántas cerraduras y cerrojos haya en tus puertas y ventanas o si tienes sistema de alarma: **si confías en la persona de la puerta que dice ser el repartidor de Amazon y le dejas entrar sin comprobar** primero si es cierto, estás ----- a cualquier riesgo.

Fuente: [ComputerHoy](http://ComputerHoy.com)