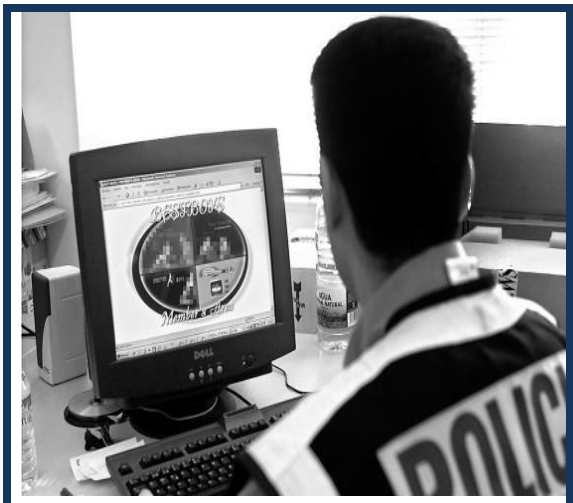

Ingeniería social – Seguridad informática.

Por Jaime Fernández Gómez
www.sindominio.com

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que “los usuarios son el eslabón débil” en seguridad; éste es el principio por el que se rige la ingeniería social.

Un ejemplo contemporáneo de un ataque de ingeniería social es el uso de archivos adjuntos en e-mails que ejecutan código malicioso (por ejemplo, usar la máquina de la víctima para enviar cantidades masivas de spam). Ahora, luego de que los primeros e-mails maliciosos llevaron a los proveedores de software a deshabilitar la ejecución automática de archivos adjuntos, los usuarios deben activar los archivos adjuntos de forma explícita para que ocurra una acción maliciosa. Muchos usuarios, sin embargo, cliquean ciegamente cualquier archivo adjunto recibido, concretando de esta forma el ataque.

Quizá el ataque más simple que aún es efectivo sea engañar a un usuario llevándolo a pensar que uno es un administrador del sistema y solicitando una contraseña para varios propósitos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación benigna; a este tipo de ataques se los llama phishing (pesca). Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores. En realidad, los administradores de sistemas informáticos raramente (o nunca) necesitan saber la contraseña de los usuarios para llevar a cabo sus tareas. Sin embargo incluso este tipo ataque podría no ser necesario — en una encuesta

realizada por la empresa InfoSecurity, el 90% de los empleados oficinistas reveló sus contraseñas a cambio de un bolígrafo barato.

Tal vez el ataque de ingeniería social a mayor escala de años recientes sea el que rodea a Messenger Plus!; para recaudar dinero con el software, su autor, Patchou, incluyó un adware de C2Media dentro del programa. Mientras que el acuerdo con el sponsor brinda la opción de instalar Messenger PLus! sin el adware, la vasta mayoría de los usuarios simplemente cliquean su aceptación del acuerdo, y por lo tanto instalan el adware innecesariamente.

La ingeniería social también se aplica al acto de manipulación cara a cara para obtener acceso a los sistemas computacionales. Entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que son seguidas es la principal defensa contra la ingeniería social.