Teléfono: 01 (33) 36 38 76 85

INGENIERIA SOCIAL

FRAUDES POR INTERNET.

Un numeroso grupo de internautas españoles recibieron hace algunos meses un correo electrónico que les confirmaba la compra en Internet de una mercancía, cargada en su cuenta corriente, que recibirían en un breve plazo de tiempo. Además de dar las gracias al supuesto cliente, la misiva indicaba que si tenía alguna duda llamaran al teléfono que aparecía al final del mensaje, donde también se atendería cualquier queja o reclamación. El número en cuestión era una especie de 906, aunque con llamada internacional, donde respondía una grabación que solicitaba unos momentos de espera a la víctima de la estafa. No había ninguna empresa al otro lado de la línea, ni compra efectuada en Internet, ni mercancía alguna que recibir. La carta era más falsa que el beso de Judas. Su objetivo: asustar al inocente para que llamara al teléfono del timador, que cobraría por cada segundo que las víctimas pasaran con el auricular pegado a la oreja.

Los métodos tradicionales de engaño funcionan en Internet a las mil maravillas. Se denominan problemas de ingeniería social para diferenciarlos de aquellos otros que se basan en cuestiones técnicas, tratados ampliamente en Criptonomicón. Los estafadores, los timadores y los embaucadores que se empiezan a acercar a la Red no necesitan apuntarse a los grupos de hackers ni leer ningún manual técnico. Las personas padecen las mismas debilidades dentro y fuera de Internet. El miedo y la codicia son patrimonio de la humanidad y los delincuentes sólo tienen que adaptar sus antiguas fórmulas al nuevo medio. El ejemplo del aviso falso de compra en la Red está basado en el miedo: el temor a perder dinero consigue que el incauto llame a un número 906. Nada tiene que envidiar la codicia, pecado muy útil en estos tiempos de nuevos ricos al instante. Los negocios increíbles crecen al mismo ritmo que el número de estafas.

¿Cuántas veces ha recibido un correo que promete 20 dólares por cada mensaje que reenvíe a sus amigos o a sus enemigos? La misiva asegura que Microsoft rastrea la red en busca de esos mensajes y regala más de 3000 ptas por cada uno de ellos. Este es un ejemplo de 'nadie gana, todos pierden'. Se pierde tiempo leyendo el mensaje, mandándolo y leyendo las respuestas de sus conocidos, algunas de ellas advirtiendo que los Reyes Magos no son los padres ni, mucho menos, Microsoft.

Unas pocas medidas profilácticas son suficientes para evitar la mayoría de los peligros que un usuario normal encuentra en la Red: una copia de seguridad reciente de los ficheros importantes, el programa antivirus actualizado y un especial cuidado en las operaciones de comercio electrónico. A la práctica habitual de estos consejos debemos añadir una buen dosis de sentido común. Los pillos que utilizan la ingeniería social para engañar al prójimo encuentran especiales dificultades cuando tratan con una persona cauta. Es posible que un internauta precavido con el aspecto social de la Red

sufra menos disgustos por causa de la seguridad que el experto en técnicas criptográficas que habla más de la cuenta en seminarios, mesas redondas o en los canales de IRC.

¿Se ha planteado alguna vez cómo robar en Internet? La alternativa basada en aspectos técnicos podría ser así: se elige un blanco apetecible, verbigracia, uno de los nuevos bancos que prestan servicio en la Red. Se consigue, con mucha discreción, toda la información posible sobre el objetivo (arquitectura de red, servidores, aplicaciones, medidas de seguridad, etc.) Se monta una maqueta que replique, a escala, el tinglado del banco en la Red. Es el momento de buscar alguna debilidad, escribir un plan de ataque y probarlo en la maqueta. Hay que localizar el rastro que se genera al cometer la intrusión y ver cómo eliminarlo. Cuando se está convencido de la bondad del plan, se pasa a la práctica real. Si todo funciona como se esperaba, el ladrón se convertirá en un nuevo rico sin haberse movido del garaje de su casa. Pero si este método le parece demasiado complejo, tenemos la segunda - que no tercera - vía: la ingeniería social.

No se elige un banco en concreto; cualquiera puede ser bueno. Seguidamente, se acude a los próximos congresos sobre seguridad, comercio electrónico y bases de datos en Internet. Se estudia con atención la lista de asistentes. Los empleados de bancos y cajas de ahorro son el principal objetivo. Durante el desayuno, los descansos o la comida, si la hubiera, hay que charlar con ellos sobre sus proyectos, instalaciones, medidas de seguridad y cualquier información que facilite la entrada a los ordenadores del banco. ¿Le parece difícil? Permítame un ejemplo personal: hace muy poco estuve en un curso de dos días en Madrid. Durante las comidas que compartí con el resto de asistentes se habló, entre otros temas, de los sistemas de protección de varias entidades financieras. Quienes comentaban estos detalles eran empleados de esas empresas. Nada demasiado importante, pero tampoco nadie buscaba especialmente esa información. O, al menos, eso me pareció a mí. ¿Hasta donde hubiera llegado un ladrón que deseara sonsacar todo los datos posibles relacionados con la seguridad de esos bancos? No sería sorprendente si al final de la jornada el supuesto delincuente supiera lo necesario para visitar los sistemas informáticos del empleado que mejor se lo pasó charlando animadamente con ese compañero de mesa tan interesado en su trabajo y sus proyectos.

Antes de terminar, quiero insistir en la necesidad de añadir a la caja de herramientas de seguridad (la misma que contiene esas fantásticas aplicaciones que nos protegen incluso de nosotros mismos) una vieja y útil cualidad de los gatos escaldados: la precaución. El hombre es un lobo para el hombre también en Internet, aunque ahora utilicemos el eufemismo de 'ingeniería social'. Sea precavido por esas redes de Dios.