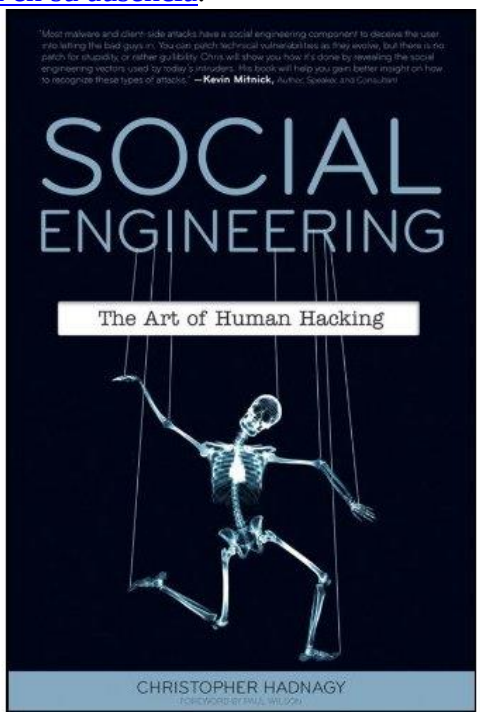
Delitos Informáticos con Ingeniería Social

Ingeniería social es un término relativamente nuevo, pero no el concepto. Para ser claros de lo que hablamos es de la picaresca, de utilizar técnicas para conseguir que una persona para que realice alguna acción o nos proporcione acceso a un sistema a través de algún tipo de engaño. Para ello no hace falta un alto conocimiento en informática, técnicamente se trata de ataques conocidos como "de bajo nivel", pero no por ello dejan de ser ataques meticulosos y efectivos.

En el mundo real, los delincuentes buscaban en tu basura, robaban tu cartera o miraban en tu escritorio. De esta forma podían encontrar tus datos de la seguridad social, DNI, cuentas bancarias, etc y realizar operaciones con ellas. En el mundo digital basta con que observen tu cuenta Facebook y averiguar el nombre de tu perro, el colegio en el que estudiaste o cualquier otro dato que se pueda usar como pregunta de seguridad en cuentas de determinados servicios en internet. O que conozcan cuando una persona se va de vacaciones y vayan a robar a su casa en su ausencia.



La buena noticia es que existen formas de limitar su actuación. De acuerdo a los expertos hay que limitar el acceso que los extraños tengan nuestros datos personales. Como perito siempre les indico a mis clientes que Internet es una proyección del mundo real, que tiene sus propias reglas que se deben conocer, pero que las bases son las mismas. De esta forma… ¿irías por la calle mostrando una foto con tu familia en la playa a todo el mundo con el que te cruzas?… si la respuesta es no, ¿por qué motivo cuelgas esa foto en Facebook sin control accesible a todo el mundo?

Por ello para evitar este tipo de ataque hay un conjunto de medidas simples y eficaces que se pueden llevar a cabo.

1.- Guarda o destruye la información impresa antes de tirarla a la basura

Personalmente ya he observado a personas en los contenedores de papel en mi localidad recuperando cartas de personas que las habían tirado a la basura sin destruir. Se debe guardar la información de forma segura o en su caso destruirla antes de tirarla.

2.- Fortalece las opciones de seguridad

Facebook y otras redes sociales ofrecen mecanismos para que la información privada permanezca privada. ¿A tus compañeros de trabajo les interesa que tu hermano haya tenido un niño? ¿Quieres comentar a todo el mundo que te vas de vacaciones y que tu casa queda vacía?, es muy sencillo configurar la privacidad para que el acceso a la información esté dirigido exclusivamente a quien debe tener acceso a esa información.

3.- ¿Es demasiado bueno para ser cierto?… pues no es cierto. Suena extraño… desconfía..

En ingeniería social utilizan dos sentimientos (o debilidades) humanas… la ambición y la compasión. ¿A quién no le gustaría comprar un teléfono móvil de última generación por 1 €?, pero lo cierto es que eso no ocurre. Te encuentras a una persona que necesita tu ayuda porque después de hablar contigo por alguna red social necesita dinero para una operación o para visitarte. ¿no parece extraño? Existen vías (servicios públicos, ONGs) a través de las cuales una persona puede recibir ayuda puntual sin tener que acudir a un desconocido.

4.- Establece unos principios de seguridad básicos y síguelos

Cosas tan obvias como no abrir correos electrónicos de extraños, no proporcionar usuarios y contraseñas por correo electrónico, etc. son precauciones que cualquier persona puede y debe seguir.

Y sobre todo, aunque no sea suficiente, utiliza el sentido común. Sin ánimo de ofender a nadie, no es muy inteligente publicar en internet una foto de tu tarjeta de crédito.

.

Autor: Carlos Pintos Teigeiro
Informática y Peritaje
http://www.informaticayperitaje.com