

Estafadores profesionales que viven de tu futuro empleo

22.05.2014
Dennis Nishi.
The Wall Street Journal

Comenzaron embaucando a incautos en las plataformas de contactos y ahora quieren vivir de la necesidad de muchos candidatos que buscan trabajo.

Cuando su antigua empresa de Seattle cerró, Stephen Graham decidió utilizar una plataforma online para buscar un nuevo trabajo. Empezó por los sitios web profesionales más populares, como Monster.com, Careerbuilder.com, Craigslist o Indeed.com, y envió a su currículum para responder a ofertas de trabajo que parecían coincidir con su experiencia laboral anterior.

Pero durante esas búsquedas online se topó con nuevos peligros. Fue entonces cuando le robaron su identidad.

Recibió una llamada de alguien que aseguraba representar a la cadena de hoteles Marriott. Su interlocutor le decía que estaba interesado en su experiencia profesional, pero necesitaba información adicional, como su número de la seguridad social, para algún tipo de verificación de antecedentes profesionales. "Todo parecía muy real", asegura Graham. "Usaban un software de reclutamiento y nada hacía sospechar". Por eso, decidió darles toda la información que requerían.

Al cabo de cuatro días, comenzó a recibir correos electrónicos de bancos en todo el país que le daban las gracias por la apertura de nuevas cuentas. Los ladrones también intentaron presentar una declaración de impuestos fraudulenta bajo su nombre.

Peligros reales

Delincuentes que resultan ser cada vez más expertos en la Red han puesto a quienes buscan empleo en su punto de mira. Muchos de ellos se hacen pasar por reclutadores y crean sitios web falsos para robar datos personales que se utilizan para cometer fraude de identidad. La consultora de investigación Javelin Strategy & Research, en Pleasanton (California), informa de que en 2013 hubo 13,1 millones de casos de robo de identidad sólo en Estados Unidos.

El simple dato de la fecha de nacimiento en Facebook es una puerta de entrada a información sobre ti.

Quienes buscan un puesto de trabajo pueden minimizar éstos y otros riesgos extremando la precaución y la diligencia acerca de con quién suelen compartir su información personal. Esto incluye también poner límites a lo que se dice y se publica en las redes sociales. Los expertos citan, por ejemplo, la fecha de nacimiento, un dato que muchos usuarios de Facebook dan sin más, y que se puede usar para acceder a otras informaciones.

Muchos estafadores aparecen bajo el disfraz de empresas reales. Por eso, antes de responder a una oferta de empleo debes comprobar que el puesto es real. Los expertos recomiendan que quienes están buscando trabajo se ocupen personalmente de gestionar su información personal.

Ten cuidado si una empresa solicita información como tu número de la seguridad social al comienzo mismo del proceso.

Se debe tener una precaución especial cuando se obtiene un contacto con un reclutador de un buscador de trabajo que parece haber salido de la nada, sobre todo si solicita información sensible. No está de más una llamada de comprobación al supuesto reclutador y verificar si éste representa a una compañía real que busca candidatos.

Investiga la información de contacto del empleador; analiza si usa servicios de correo electrónico o direcciones genéricas como Hotmail; si aparece el nombre de la compañía en la home page... Puedes utilizar herramientas como Whois (<http://whois.net>) para verificar que la empresa tiene un sitio web real. Debes asimismo estar atento a los dominios de nueva creación con "matrícula" extranjera.

Del mismo modo, es conveniente que cambies con frecuencia tus contraseñas en aquellos portales de empleo o bolsas de trabajo en los que te hayas registrado. Los hackers tienen capacidad para acceder a fragmentos de datos cifrados.

Un decálogo de engaños

Algunas ofertas falsas aprovechan las dificultades para encontrar empleo para engañar con oportunidades laborales que no llegan a efectuarse. Facua-Consumidores en Acción advierte de su aumento y ha elaborado un 'top ten' con las más comunes:

1. Ofertas para trabajar de canguro o cuidador en el extranjero a cambio de tener que pagar una cuota.
2. Ofrecer un trabajo a través de distintas vías, entre ellas correos electrónicos o spam. Se solicita al usuario que ingrese en una cuenta bancaria una cantidad para gastos del contrato o del envío del material. Tras abonar lo que se le pide, la empresa desaparece o incluso vuelve a contactar con el afectado para seguir solicitándole dinero.
3. Correos electrónicos o SMS que, en vez de pedir un pago, pretenden captar los datos de los usuarios para incluirlos en listas de spam. Se envían los datos a listas de publicidad masiva, e incluso puedes ser víctima de ataques de seguridad.
4. Se promete ganar dinero rellenando encuestas, con un ingreso extra desde casa. Pero el acceso a estos cuestionarios no es gratis.
5. Facua ha denunciado varios anuncios de trabajo entre los que se encuentra una oferta que solicita "jornaleros para diversas campañas de recogida de fruta". Para ponerse en contacto con el supuesto demandante señala "para más información pregunten por Claudia al teléfono 668803593". Al llamar al número indicado una locución remite al número de tarificación adicional 806514296 e insiste en la necesidad de ponerse en contacto por esta vía. La llamada a este teléfono 806 tiene un coste por minuto desde redes fijas entre 0,91 euros y 1,21 euros; y desde dispositivos móviles, entre 1,27 euros y 1,57 euros, IVA incluido.
6. "Hágase rico, o casi, fabricando productos desde casa". El dinero que se solicita es el teórico coste del material con el que el usuario se dedicará a fabricar productos desde casa para venderlos a través de la empresa.
7. Determinadas academias muestran en su publicidad la falsa promesa de que el usuario encontrará empleo en cuanto finalice uno de sus cursos por sus supuestas relaciones con empresas.
8. Negocios piramidales en los que el supuesto trabajador debe comprar productos a la empresa para revenderlos captando nuevos empleados. Los afectados son clientes de la compañía que intenta convencerles de que se harán ricos en breve.
9. Hacer creer al usuario que ganará dinero actuando como mediador en transacciones internacionales. Para ello debe recibir transferencias en su cuenta bancaria y reingresar el dinero en otro número de cuenta quedándose con una comisión.
10. Se publicita una oferta en la que el "empleado" no va a tener ninguna remuneración. Entre los requisitos está la alta cualificación, la calidad del trabajo que realice y la seriedad en los plazos del mismo.