¿Cómo evitar estafas y suplantación de identidad en LinkedIn?

Con la llegada de la internet las redes sociales han tomado un papel principal en las actividades diarias. Un claro ejemplo es LinkedIn, la cual está enfocada al mercado laboral. A pesar de su éxito, se vienen presentando denuncias por estafa.

Según ECommerce Times, LinkedIn no solo se habría convertido en uno de los objetivos principales de las campañas de phishing de Internet, sino que habría recibido más de la mitad de todos los ataques phishing a nivel mundial, en el primer trimestre del 2022.

Al conocer la magnitud, **Selva Orejón, docente de EAE Business School**, aclara algunas dudas sobre la suplantación de identidad, donde explica: ¿qué es el phishing?, a quién acudir en caso de ser suplantado y ¿cómo evitar ser víctima de ello? Y cómo detectar un perfil falso:

¿Qué es el phishing y a quién acudir si ha sido víctima?

El **phishing** es una técnica empleada por delincuentes informáticos con la intención de engañar, estafar y robar información de usuarios en la red, normalmente contraseñas, números de tarjetas de crédito, entre otros.

En algunos casos estas personas suelen suplantar la identidad de personas u organizaciones para hacer llegar sus mensajes a las víctimas, parezcan reales y las personas acaben facilitando dicha información. También pueden crear perfiles falsos en **LinkedIn**, suplantando la identidad de una persona u organización.

La acción más frecuente es la suplantación, la cual hace para realizar estafas económicas, dañar la reputación de la víctima enviando mensajes falsos. En el caso de LinkedIn, en concreto, hacerse pasar por empresas o reclutadores con el fin de conseguir su objetivo: estafar bajo el contexto de conseguir trabajo, condiciones laborales mejores, etc.

Las ofertas laborales falsas en países de Latinoamérica son frecuentes. Supuestas empresas y reclutadores prometen empleo de manera rápida con una cantidad de dinero que deben dar antes de ingresar u ofreciendo condiciones de contratación diferentes a las pactadas en la vacante.

Notificaciones falsas

En LinkedIn la táctica más usada es el envío de notificaciones falsas, por medio de la cual el victimario envía correos electrónicos haciéndose pasar por LinkedIn, empleando asuntos atractivos como “Apareciste en tres búsquedas esta semana” o “Felicita a Juan por su nuevo trabajo”.

Estos mensajes, en su mayoría, son acompañados de un enlace, o link, en donde el usuario termina ingresando su correo y contraseña, entregando así el acceso a su cuenta a los atacantes (y a las otras en las que use las mismas credenciales).

Vale la pena resaltar que estos ciberataques no solo buscan dinero, pueden estar interesados en adelantar acciones de espionaje, enviando archivos infectados con los que pueden infiltrarse en la red de las compañías.

Es importante tener claro que si usted es **víctima** de una suplantación debe recurrir de inmediato ante la Fiscalía o policía nacional, esto por tratarse de un delito de falsedad personal, el cual está plasmado en el artículo 296 del código penal.

¿Cómo evitar suplantación de identidad en LinkedIn u otras redes sociales?

Para evitar suplantación de identidad es clave no proporcionar información personal, tener el perfil privado, aceptar solicitudes de personas cercanas o conocidas, no pinchar en enlaces sospechosos ni proporcionar datos sensibles como: cédula, números de tarjetas de crédito o débito, ni consignar dinero a menos de estar seguro de realizar dicha transacción verificando la autenticidad del portal y si somos personas públicas tratar de verificar nuestros perfiles en redes

sociales.

Y siempre que lo detectemos se ha de poner en conocimiento de la plataforma y de las autoridades policiales.

Otra recomendación es, si recibe correos de dudosa procedencia o un desconocido se pone en contacto con usted que no sea legítimo, no haga clic en ningún enlace. Pregunte siempre "¿cómo me encontró esta persona? ¿Por qué me contactan?"

Esta aplicación también permite que usted cuente con doble verificación, esto hará que, cada vez que inicie sesión, usted sea notificado por correo o en un mensaje de texto a su móvil. Y, por último, pero no menos importante, recuerde que las ofertas de trabajo reales cumplen con las leyes fiscales y del país. El dinero fácil tiende a ser una estafa.

Las **redes sociales** más vulnerables a suplantación son: Instagram, Facebook, Tinder, Onlyfans, Telegram y como lo mencionamos al inicio **LinkedIn** con ofertas falsas de trabajo.

¿Cómo puedo detectar un perfil falso en redes sociales?

La profesora de **EAE Business School**, Selva Orejón, recomienda siempre buscar el nombre en cada red social para verificar si hay perfiles similares, desconfiar si el perfil es reciente,

tiene pocos amigos, faltas de ortografía y sospechar aún más si solicita información. Es clave buscar otro canal de comunicación de la persona o empresa para confirmar.

"*El mundo de las redes sociales está en constante evolución, y permiten tener información básica a la mano, por eso ahora es más fácil la autenticación de un perfil o confirmar si la información es real o falsa*", enfatiza la profesora de EAE Business School, Selva Orejón.

Para nadie es un secreto que **LinkedIn** es de gran atractivo para el mundo laboral, al ser una plataforma útil. Por eso la profesora de EAE Business School brinda 5 consejos para potencializar su perfil profesional:

1. Tu fotografía refleje tu esencia que sea natural, pero sería que esta es una plataforma profesional, evita los selfies y fotografías de fiesta.
2. En la descripción explica detalladamente tus aptitudes y habilidades, recuerda usar palabras clave en la descripción.
3. Mantén el perfil siempre actualizado y procura que tus anteriores responsables validen aptitudes de tu perfil, esto último generará confianza
4. Interactúa diariamente en la red ofreciendo contenidos que sean de interés y crecimiento personal y profesional
5. Aprovecha los cursos gratuitos de la red social y continúa preparándote para nuevos retos profesionales