## Cómo tu LinkedIn puede ayudar a los delincuentes a cometer delitos

## *ESET, compañía de seguridad informática, advierte que los ciberdelincuentes pueden interactuar mediante perfiles falsos en esta plataforma y obtener tus datos de manera sencilla con fines maliciosos, e incluso generar ataques dirigidos a tu empresa.*

Hay varias formas en que los delincuentes pueden obtener información personal de los usuarios como número de teléfono móvil o dirección de correo electrónico, la principal es a través de filtraciones de datos que ocurrieron en distintos sitios web que son vendidos entre los delincuentes. Pero desde [ESET](https://www.eset.com/latam/), compañía líder en detección proactiva de amenazas, advierten que sin el uso adecuado, Linkedin, una de las redes sociales más utilizadas en la actualidad, es también una gran fuente de información para los ciberdelincuentes.

*“LinkedIn tiende a ser usada con fines profesionales, y los usuarios intentan aumentar su red para obtener contactos o posibles propuestas profesionales. Con esto en mente, muchos de sus usuarios configuran sus perfiles para que sean receptivos y llenos de información de contacto, y los delincuentes sin duda lo aprovechan.”,* comenta Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Un delincuente, sin necesidad de comprar un listado de información filtrada, solo necesitaría usar uno de los *Web Crawlers* (software automatizado que navega por la Internet de manera metódica y automatizada con el fin de  indexar información sobre sitios web y sus contenidos) para LinkedIn, y recopilar así toda la información de contacto disponible de sus objetivos. Además, puede que la intención no sea solo engañar al usuario del cual se obtuvo la información, sino que podrían buscar atacar la empresa en la que trabajan. De esta maneta la información obtenida podría resultar en un ataque más efectivo, ya que los ataques digitales personales podrían tener características distintas.

Entre las posibilidades de obtención de datos que realiza el *Web Crawler*, se destacan dos que pueden obtener datos específicos:

* **Creación de una lista de los empleados actuales de la empresa:** En este caso, lo único que tiene que hacer el delincuente es configurar el software de recogida para que vaya a la pestaña “Personas” de la empresa objetivo. Esto dará como resultado una lista de empleados muy actualizada, ya que es casi un procedimiento estándar realizar cambios en la red social para mostrar dónde se trabaja actualmente.
* **Lista de objetivos de la cadena de suministro relacionados con el objetivo:** Además del esfuerzo inicial de recopilación, es posible repasar las interacciones realizadas en los posts de la empresa para identificar posibles proveedores y socios, obteniendo así nuevos objetivos principales o posibilidades de atacar la cadena de suministro del objetivo inicial.

Al examinar con más detalle las posibilidades de recopilación de datos, los delincuentes se enfrentarían básicamente a tres formas diferentes de proporcionar información. Desde ESET destacan que es importante recordar que las formas mencionadas pueden ser reveladas al público en general o ser más restringidas, siendo reveladas solo a aquellos que pertenezcan a la lista de contactos:



Pie de imagen: Acceso a la información de contacto para personas fuera de la red de conexiones.



Pie de imagen: Acceso a la información de contacto para personas fuera de la red de conexiones.

**Perfiles que no proporcionan ningún dato:** Elegir no proporcionar ningún dato de contacto fuera de la plataforma significa que el número de informaciones que pueden recopilar los delincuentes se reduce considerablemente. Aun así, a menudo son capaces de recopilar datos como el nombre completo, el puesto de trabajo y la región en la que se encuentra la empresa.

**Perfiles que solo proporcionan una dirección de correo electrónico de contacto:** Aunque LinkedIn es una red enfocada a proporcionar información de contacto personal, algunos usuarios también proporcionan su dirección de correo electrónico corporativa actual. Independientemente del correo electrónico que se facilite, esto permite a las personas malintencionadas llevar a cabo interacciones más específicas con sus víctimas. Según ESET, uno de los posibles agravantes de facilitar la dirección de correo electrónico corporativa es que los delincuentes sabrán con certeza cómo se componen los correos electrónicos pertenecientes a la empresa. La mayoría de las empresas utilizan el formato estándar “nombre.apellido@empresa.com” o variaciones del mismo, como la primera letra del nombre seguida del apellido o todas las iniciales, además del apellido escrito completo. Disponer de esta información ahorra tiempo a los delincuentes.



Pie de imagen: Información de contacto de personas añadidas previamente a la red de conexiones.

**Perfiles que facilitan números de teléfono:** De las opciones mencionadas anteriormente, proporcionar números de teléfono es sin duda la más crítica, porque además de permitir interacciones en tiempo real, los delincuentes pueden recopilar estos datos para [venderlos en forma de lista de clientes](https://www.welivesecurity.com/la-es/2021/04/08/comercializan-datos-500-millones-usuarios-linkedin/) o algo equivalente.

**¿Cómo proteger los datos?**

La propia naturaleza de este tipo de interacciones en las redes sociales, sean cuales sean, permite a los delincuentes acceder a algunos de los datos si tenemos perfiles registrados en ellas. Aun así, hay algunas medidas que se pueden tomar para evitar que los delincuentes accedan a información más valiosa. ESET comparte la siguiente:

* **Configurar la privacidad en LinkedIn:** Existen varias opciones de privacidad que ayudan a evitar que personas malintencionadas interactúen con éxito. La principal es configurar la red para que no dé demasiada información a nadie que no pertenezca a la lista de contactos. Y conviene recordar que este consejo se aplica a todas las redes sociales.
* **Ser juicioso:** De nada sirve configurar correctamente todas las opciones de privacidad y seguridad si se acepta cualquier solicitud de contacto sin ningún criterio. Hay muchos bots y perfiles falsos registrados en la red, así que es importante establecer criterios antes de aceptar una conexión.
* **Limitar la cantidad de información que el sistema tiene sobre ti:**Al tratarse de una red social, la propia plataforma ya permite que se produzcan interacciones entre los usuarios, ya sea para contactar o para ofrecer/buscar oportunidades laborales. Considerar priorizar el contacto a través de las herramientas que proporciona la plataforma y evitar proporcionar datos externos.
* **Evaluar** **las conexiones:** Ya hay muchos perfiles falsos circulando por la red, revisar periódicamente la lista de conexiones y limpiar aquellos contactos que parezcan sospechosos.
* **Evaluar si la información en tiempo real es esencial**: Analizar si es realmente necesario cambiar el estado del lugar donde se trabaja el mismo día que se empieza. Algunos delincuentes vigilan activamente este tipo de cambios y pueden aprovechar el escaso conocimiento del entorno para enviar contenido malicioso.

Para conocer más sobre seguridad informática visite el portal de noticias de ESET: <https://www.welivesecurity.com/es/consejos-seguridad/como-linkedin-ayuda-delincuentes-cometer-delitos/>

Por otro lado, ESET invita a conocer [**Conexión Segura**](https://www.eset.com/latam/podcast/), su podcast para saber qué está ocurriendo en el mundo de la seguridad informática. Para escucharlo ingrese a: <https://open.spotify.com/show/0Q32tisjNy7eCYwUNHphcw>

**Visítanos en:**

  [@ESETLA](https://twitter.com/ESETLA)  [/compay/eset-latinoamerica](https://www.linkedin.com/company/eset-latinoamerica/)  [/esetla](https://www.instagram.com/esetla/)  [/ESETLA](https://www.facebook.com/ESETLA)  [/@esetla](https://www.youtube.com/%40esetla)

**Acerca de ESET**

Desde 1987, ESET® desarrolla soluciones de seguridad que ayudan a más de 100 millones de usuarios a disfrutar la tecnología de forma segura. Su portfolio de soluciones ofrece a las empresas y consumidores de todo el mundo un equilibrio perfecto entre rendimiento y protección proactiva. La empresa cuenta con una red global de ventas que abarca 180 países y tiene oficinas en Bratislava, San Diego, Singapur, Buenos Aires, México DF y San Pablo.

**Datos de Contacto de Comunicación y Prensa**

*Para más información se puede poner en contacto a través de* ***prensa@eset-la.com*** *o al +54 11 2150-3700.
Además, puede visitar “Somos ESET” nuestro Blog de Comunicación de ESET con las últimas novedades, disponible en:* [*https://www.somoseset.com/*](https://www.somoseset.com/)

*Copyright © 1992 – 2023. Todos los derechos reservados. ESET y NOD32 son marcas registradas de ESET. Otros nombres y marcas son marcas registradas de sus respectivas empresas.* 

