Fuente:
IT Connect

A diferencia de otras redes sociales, LinkedIn está orientada al ámbito empresarial y al networking.

Esto ha hecho que se diferencie del resto y ha contribuido al gran aumento de su popularidad. Sin embargo, como ocurre en muchos casos, mientras más popular sea una red social, mayores son las probabilidades de tener problemas de seguridad.

La popularidad de esta red social ha llevado a los expertos de Kaspersky Lab a reflexionar sobre la manera en la que utilizamos y en la cantidad y el tipo de contenido que compartimos.

A la hora de crear una nueva cuenta, la mayoría de los usuarios marcan casillas y aceptan los términos y condiciones sin una lectura previa, dejando a un lado el nivel de configuración de privacidad de la información profesional que van a compartir. Es por esto que Kaspersky Lab ofrece los siguientes consejos de privacidad, seguridad y uso de contraseñas para disfrutar de la aplicación y compartir los contenidos de una manera segura:

Contraseña. El uso de contraseñas fuertes es vital. Para asegurar la protección de tus cuentas, cambia tus contraseñas regularmente y no las reutilices. Pero, además, es muy importante contar con contraseñas fuertes que sean difíciles de averiguar. Si no tienes claro si tu contraseña es lo suficientemente fuerte, siempre puedes comprobarlo usando la herramienta Kaspersky Secure Password Check.

Privacidad. El perfil de los usuarios en esta red social contiene una gran cantidad de información personal, por lo que es muy importante configurar los ajustes de privacidad de tu cuenta y asegurarte de que está realmente protegida.
Para controlar quien puede ver la información que compartes en tu feed de LinkedIn, selecciona “Quién puede ver el feed de tu actividad”. En este caso, te recomendamos seleccionar la opción “Tus contactos”, que es la que aparece por defecto. Esto significa que solo tus contactos, a quienes has aceptado previamente, pueden ver la actividad de tu perfil. Además, existe la opción “Edita tu perfil público” que te permite seleccionar lo que pueden ver las personas que no están conectadas a tu perfil.

También puedes limitar quién puede ver tus contactos. Al estar relacionado con mucha gente de forma pública, puede ser más fácil encontrar más información sobre ti. Escoger la opción de que solo tú puedas ver tus contactos puede ayudarte a proteger tu privacidad.

Por último, la configuración predeterminada de LinkedIn permite que otras personas sepan cuándo has visto sus perfiles. Sin embargo, lo más probable es que no quieras que la gente sepa cada vez que ves su perfil, por

lo que puedes cambiar esta opción para permanecer anónimo.

Seguridad. Puede ser que te veas tentado a la idea de conectar con el mayor número de personas posible para ayudarte a encontrar un trabajo. Aunque esto pueda ser de ayuda hasta cierto punto, no deberías agregar a tus contactos a gente que no conoces de nada. Lo creas o no, hasta LinkedIn tiene hackers. Estos usan cuentas falsas para ganarse la confianza de los representantes de algunas empresas y atacarlos a ellos o a sus negocios. Así que, si recibes una solicitud de contacto de alguien de quien no has oído hablar nunca, te recomendamos que hagas clic en “ignorar”.

Si recibes una solicitud de alguien que no conoces, pero podría proporcionarte una buena oportunidad de trabajo, deberías al menos investigar su perfil y ver si algo no encaja.

Si descubres que alguien está usando un perfil falso, sobre todo si es un perfil en el que se hacen pasar por ti, infórmalo inmediatamente. Para hacerlo, haz clic en la pequeña flecha que aparece junto a la opción “Enviar un mensaje” en el perfil personal en cuestión, luego haz clic en “Bloquear o denunciar” en la lista desplegable.
Desde aquí, haz clic en “denunciar” y selecciona la razón por la que quieres denunciar este perfil. También puedes aportar más información si lo consideras necesario. LinkedIn comprobará esta cuenta y si determina que es un perfil falso, la eliminará.

LinkedIn también ha sido objeto de un gran número de mensajes fraudulentos y de phishing. Estos mensajes suelen ofrecer oportunidades de trabajo fantásticas pero, al final solicitan algún tipo de información financiera del usuario. Nunca proporciones tus datos financieros a un desconocido en LinkedIn. Y si recibes un mensaje que parece spam, ponte en contacto con LinkedIn rápidamente para informarles al respecto.

Disponible en:

http://itconnect.lat/latinoamerica/3623 [1]

Links
[1] http://itconnect.lat/latinoamerica/3623