LinkedIn, the risks of keeping your professional profile online

Translated by Content Engine LLC . CE Noticias Financieras , English ed.; Miami [Miami]. 20 Oct 2021.

FULL TEXT

It's very important for users to pay close attention to privacy settings when signing up for a social network, whether it's Facebook, Instagram, TikTok or even LinkedIn.

Whether you are working from home or holding a position in a company, the professional social network is suitable for everyone. Not only can you get a job through it, but it lets your network know who you are, what you do and all your professional accomplishments and preferences.

Users upload their CVs online and establish different business relationships, either between people or companies. Look for work synergies and new business opportunities.

Julio Seminario, Bitdefender's IT security expert in Peru, points out that LinkedIn offers job opportunities and contacts with more than 750 million professional profiles.

"However, maintaining a complete professional profile in the online world has its difficulties. As with any social networking service, your profile is vulnerable to privacy and security issues, including data tracking and hacking," warns Seminario.

While some of the information that is made public may not pose an immediate risk, he says users should be aware of long-term privacy concerns.

"The data you share online will circulate outside of your social network, regardless of how many security measures you or the platform have implemented," the security expert mentions.

"Making small privacy tweaks when setting up your network can help protect you against complex social engineering schemes like phishing and scams," he adds.

He also recommends being mindful of connections. "Take a moment to think before accepting a connection request from people you don't know."

Recommendations to keep in mind:

Use a unique and complex password to log into your account (numbers and letters, upper and lower case, for example) and enable two-factor authentication.

Beware of people who communicate with you through direct messages and never click on links they send you.

Stick to the "too good to be true" rule. If something seems crazy, it probably is.

Install a security solution with anti-phishing and anti-fraud protection to block suspicious websites.

Seminar highlights that cyber thieves are actively targeting users through phishing attacks designed to mimic legitimate correspondence from the two popular web-based platforms.

One phishing attack detected on June 24 appears to have originated in the United States.

"Thirty-three percent of the fake emails reached users in the U.S., 26 percent in Ireland, 14 percent in Korea, 12 percent in Sweden, 5 percent in Denmark, and 1 percent in Finland, the U.K. and India. This fraudulent email, disguised as automated Microsoft SharePoint sought to steal the login credentials of its targets."

"Most of the emails use COVID-19 as a ruse to trick recipients into accessing a fake document," detailed the Bitdefender executive in Peru.

In that line, he explains that there are emails requesting to review a "Covid 19 help fund approved by the board of directors".

Users who try to access the document will be directed to a landing page that mimics an Outlook login page. Those who fall for the hoax are giving the attackers their legitimate Microsoft credentials.
"Users should be vigilant and verify correspondence before downloading an attachment or providing login credentials, which gives cybercriminals the advantage and freedom to access sensitive information," concludes Seminario.
CREDIT: CE Noticias Financieras English - CENFENG

DETAILS

Subject:	Internet crime; Security management; Privacy; Social networks
Business indexing term:	Subject: Social networks; Corporation: LinkedIn Corp
Location:	United States--US Peru
Company / organization:	Name: LinkedIn Corp; NAICS: 518210
Publication title:	CE Noticias Financieras, English ed.; Miami
Publication year:	2021
Publication date:	Oct 20, 2021
Publisher:	ContentEngine LLC, a Florida limited liability company
Place of publication:	Miami
Country of publication:	US Minor Outlying Islands, Miami
Publication subject:	Business And Economics
Source type:	Wire Feed
Language of publication:	English
Document type:	News
ProQuest document ID:	2584245285
Document URL:	https://www.proquest.com/wire-feeds/linkedin-risks-keeping-your-professional-profile/docview/2584245285/se-2?accountid=44910
Copyright:	CE Noticias Financieras English, Latin America - Distributed by ContentEngine LLC
Last updated:	2021-10-22
Database:	ABI/INFORM Collection