The 1,000 Chinese SpaceX engineers who never existed

LinkedIn users are being scammed out of millions of dollars by fake connections posing as graduates of prestigious universities and employees at top tech companies.

By Zeyi Yang

If you were just looking at his LinkedIn page, you'd certainly think Mai Linzheng was a top-notch engineer. With a bachelor's degree from Tsinghua, China's top university, and a master's degree in semiconductor manufacturing from UCLA, Mai began his career at Intel and KBR, a space tech company, before ending up at SpaceX in 2013. Having spent the past eight years and nine months working in the human race to space, he's now a senior technician.

Except all is not as it seems.

Upon closer inspection, there are plenty of red flags: Despite having been in the US for 18 years, Mai has written all his job titles, degrees, and company locations in Chinese. His bachelor's degree is in business management, even though his alma mater, Tsinghua, only offers that degree to student athletes, and Mai was not one. Besides, the man in his profile photo looks younger than Mai's stated age. The image, as it turns out, was stolen from Korean influencer Yang In-mo's Instagram. In fact, none of the information on this page is true.

The profile of "Mai Linzheng" is actually one of the millions of fraudulent pages set up on LinkedIn to lure users into scams, often involving cryptocurrency investments and targeting people of Chinese descent all over the world. Scammers like Mai claim affiliation with prestigious schools and companies to boost their credibility before connecting with other users, building a relationship, and laying a financial trap.

Since last year, such activities have been steadily on the rise on LinkedIn, following years of proliferation on other social media platforms and dating apps. In the second half of 2021, LinkedIn removed 7% more profiles because of fraudulent identities than in the six months before that, according to Oscar Rodriguez, LinkedIn's senior director of trust, privacy, and equity. "Scammers are highly sophisticated and proactive in terms of how often they adapt tactics," he says. For instance, a week after the Biden administration announced its student loan forgiveness plan, LinkedIn started seeing scammers incorporating the news into their scripts.

By now, victims have lost millions of dollars through scams that originated on the platform. This summer, the FBI announced it would investigate these scams and work with victims to identify the bad actors and disable their accounts, even though the financial losses are almost impossible to recover.

Scammers "are always thinking about different ways to victimize people, victimize companies," Sean Ragan, the FBI's special agent in charge of the San Francisco and Sacramento field offices, told CNBC in June. "And they spend their time doing their homework, defining their goals and their strategies and their tools and tactics that they use." He called the work of these criminals a "significant threat."

A SpaceX "employee" invited you to connect

At one point in July, there were over 1,000 LinkedIn profiles for individuals who, like "Mai Linzheng," claimed to have graduated from Tsinghua University and to work at SpaceX. The eye-popping number even triggered patriotic Chinese influencers to lament the brain drain and accuse Chinese university graduates of disloyalty to their country.

This caught the attention of Jeff Li, a Toronto-based tech influencer and columnist at Financial Times China. He confirmed on July 11 that he could find 1,004 Tsinghua graduates by searching for SpaceX employees on LinkedIn; this would have made the alumni group the largest at the company. But many accounts he saw claimed the exact same education and work experiences—suggesting that someone was mass-generating fake profiles.

"They all graduated from Tsinghua and went on to the University of Southern California or similar well-known universities," Li says. "Besides that, they all worked at a certain company in Shanghai. Obviously, I suspect these are fake, generated data."

(SpaceX did not reply to a request from MIT Technology Review asking to confirm the number of Tsinghua graduates working at the company.)

This wasn't the first time Li had noticed what he thought were fake LinkedIn accounts. Starting in late 2021, he says, he started seeing profiles with under a few dozen connections—rare for real users—and with profile photos that were always good-looking men and women, likely stolen from other websites. Most appeared to be of Chinese ethnicity and to live in the United States or Canada. In recent years, as China has cracked down on fraudulent online activities, these operations have pivoted to targeting people elsewhere who are of Chinese descent or speak Mandarin. The Global Anti-Scam Org (GASO) was established in July 2021 by one such victim, and the organization now has nearly 70 volunteers on several continents.

While these fake accounts are relatively new to LinkedIn, they have permeated other platforms for a long time. "Scammers started moving to LinkedIn maybe after dating sites tried to crack down on them,

LinkedIn scammers may target people of Chinese descent by claiming similar experiences or affiliations.

STEPHANIE ARNETT/MIT TECHNOLOGY REVIEW

[like] Coffee Meets Bagel, Tinder," says Grace Yuen, a GASO spokesperson.

In certain ways, LinkedIn is a great way for fraudsters to expand their reach. "You might be already married and you are not on the dating sites, but you probably have a LinkedIn account that you check occasionally," says Yuen.

A scammer on LinkedIn may try to connect with someone through common work experience, a shared hometown, or the feeling of living in a foreign country. Over 60% of the victims who have reached out to GASO are Chinese immigrants or have Chinese ancestry, which these actors lean on to evoke nostalgia or a desire for companionship. The fake claims to have graduated from China's top universities, which are notoriously difficult to get into, also help scammers earn respect.

On average, LinkedIn victims in particular tend to lose more money than victims of fraud on other platforms—oftentimes over a million dollars, says Yuen.

"Unlike dating sites, which are where the first scam victims were coming from, LinkedIn actually has a lot of information that's really useful for the scammers," she says. "They know your earning potential based on the type of work you listed."

The responsibility for preventing these scams, though, also falls on the sites where perpetrators hunt for their victims in the first place. After several media reports about the rampant scams on LinkedIn, the platform released a report in June that says it has been able to detect 96% of fake accounts before the people behind them make any contact with users.

LinkedIn does this through a mix of algorithms, industry expert suggestions, and human user reports, says Rodriguez. It looks for behavioral signals, like whether a new account immediately starts to message other users, and whether any of these users block or flag the account. To LinkedIn's credit, Li, who confirmed the presence of fake SpaceX engineers on the platform, says this year he has noticed that scam accounts are being taken down more quickly. "At the end of last year, the account might survive three or four days; now they're being taken down in hours," he says.

But anyone who searches LinkedIn today for SpaceX employees who graduated from Tsinghua University is still likely to find around 200 results—including "Mai Linzheng" and other fakes. Generally speaking, Rodriguez explains, the platform prioritizes identifying fake accounts that are actively engaging with real users; accounts that remain could have been dormant after registration. *To read the full story, visit www.technologyreview.com.* ■