

That Great Job Offer? It May Be a Scam

Fake offers are showing up on LinkedIn, Indeed and other employment-search sites. And they are costing the victims a lot of money.

By Heidi Mitchell – Wall Street Journal – September 9, 2021, page R2

Around Christmas last year, Sarah Magno, a 27-year-old freelance digital-media editor in Jackson Township, N.J., received a text from somebody who said he was Devon McCoy, a hiring manager for the Humane Society for Tacoma-Pierce County in Washington state. It was welcome news: Ms. Magno had applied for a remote full-time position on dozens of job sites.

Sent to the cellphone number Ms. Magno had put on her résumé, Mr. McCoy's text suggested she speak via an app with a man who is listed as a board member on the Humane Society's website. He told her how to contact the board member, who then sent her a long list of questions, such as, "How do you work under pressure?" and, "If you've made a mistake with a client, how do you confront them?" says Ms. Magno. Over two weeks, Ms. Magno connected with other people who used what looked like legitimate Humane Society email addresses, and was eventually offered a job for \$30 an hour plus benefits.

But before starting, her new bosses told her that she would need a company-issued laptop and printer, for which they'd pay. They sent Ms. Magno two digital checks

around the first of the year. They also told her that she needed to get other supplies from specific vendors, and that they would reimburse her the money.

Then things got suspicious. "There would be little hiccups, like they needed me to front \$500 because they miscalculated what DHL charged for shipping," she says. "If I didn't get the supplies on time, they threatened to push back my start date." They also messaged her about potential projects she'd be working on, which kept her enthusiasm up.

NEWSLETTER SIGN-UP

The 10-Point.

A personal, guided tour to the best scoops and stories every day in The Wall Street Journal.

PREVIEW
SUBSCRIBE

After two weeks, Ms. Magno's bank informed her that the two checks had bounced—after she had sent around \$7,000 from her personal account to the vendors. It turns out the real Humane Society hadn't posted the job, and nobody named Devon McCoy even

works there, according to a spokeswoman for the nonprofit. And the vendors they told her to deal with were phony.

“I think I knew early on this wasn’t a real job,” Ms. Magno says, “but I had to find a job as quickly as I could. I wanted to believe.”

Scam tracking

Move over, Nigerian princes. According to the Federal Bureau of Investigation’s Internet Crime Complaint Center, more than 16,000 people in the U.S. reported being victims of employment scams in 2020, with losses nearing \$60 million. The Better Business Bureau’s [2020 Employment Scams Report](#) estimates that the median dollar loss per victim of such cons last year was \$995. Tim Ball, the former director of cybersecurity at the data and analytics company Civis Analytics, says that nearly all employment scams follow a similar pattern: Criminal organizations create fake postings on job boards; they conduct fake interviews with victims via an encrypted messaging app; they get applicants’ mailing addresses and send them bad checks; they have the people being scammed deposit those checks that often bounce, but also have them use their own

money to “buy” products from preferred “vendors”—products that never show up from vendors that don’t really exist.

“At the end of the day, what we’re talking about is an old trick: These are confidence artists,” Mr. Ball says. “They may be using a computer, but these aren’t sophisticates trying to run malware. They will just say, Hi, I can offer you your dream job, I just need your address.”

No demographic is immune. “A lot of people think that only older people get scammed, but the average age of those who were most exposed and susceptible to an employment scam in 2020 was 25 to 34,” says Luke Frey, a BBB spokesman. “These scammers are smart and clever and are always finding new ways to take advantage of anyone at any age.”


Though some scammers do embed malware into faux interview emails in hopes that the applicant uses a work-issued computer or email address, the typical swindler doesn’t need to. “They may take your personally identifiable information and sell it to another team that specializes in identity theft,” Mr. Ball says. “But usually they disappear once they get their payoff.”

Fake Job Offer Primer

Here are a few clues you have been sent a fake job offer by email:

The image shows an email interface with a header bar containing icons for back, flag, trash, and folder. The email content includes a subject line, sender information, a logo, and several paragraphs of text. Red callout boxes point to specific parts of the email, highlighting red flags. The text in the email is as follows:

Sub: JOB OPPORTUNITY
Today at 10:52 PM
From: Awesome Computer Systems Corporation
To: Applicant
Cc:
Company Doc


Awesome Computer Systems Company

Dear Applicant,

I am very happy to inform you that our HR Dept has reviewed your resume and you have made it to the next step. this is a work at home job. All you will need is an hour or two to carry out the job each day. Your wages will be 400 USD per week.

We are pleased to invite you to an Online Interview for the position. Our Personnel Manager will brief you further concerning the company and the position. The interview session will be conducted online via Telegram Messenger app.

Please be advised that you will need to set up an account with Telegram. Also, the company will need to run a background check on you for a small fee.

Kindly get back to us with your **PHONE NUMBER AND PERSONAL EMAIL IF YOU ARE INTERESTED IN THE JOB POSITION** and we will give you further instructions.

Regards,
John Smith
Recruiting Manager
Awesome Computer Systems Corporation

Red flags

- The email doesn't come from a company domain. Mouse over and click on the email address to expose the full domain, then search for it online; if it looks suspicious, ask for the person to send an email from a company account. Cross-check the sender's name with their profiles on job boards to confirm their identity.
- Grammar is off, and there is no indication of what the job entails.
- The job is too good to be true (e.g. too much money for little work; extremely flexible hours; etc.) Search for the company online and call its HR department to see if the job is real.
- Recruiter asks you to "switch channels" to an end-to-end encrypted app such as Telegram, Signal or WhatsApp. Gently request a video interview, explaining that you'd like to see your future employer.
- You are told the company needs to run a background check that you will need to pay for—or that the recruiter needs to collect her fee from you or that the company will need you to cover the expenses for office equipment. If you proceed, ask if the company will pay.

Red flags

There are lots of red flags to watch for when applying for a job, cybersecurity experts say. Receiving an email from a free account is one, though many criminals will “typo-squat,” or buy domain names similar to the company supposedly doing the hiring.

“Always click on the sender’s email address to see the full name, and if it seems suspicious, ask them to email you from their work account,” says Julia Pollak, chief economist at the job

site [ZipRecruiter](#). ZIP 3.68%

Since many employment swindlers are foreign and are pasting copy from a well-worn script, poor grammar and misspelled words are usually giveaways, as are big promises like “no interview necessary” or “instant hire.” Offering exorbitant money in exchange for little work should tip off job seekers, says Ms. Pollak. She advises people to cross-check the recruiter’s name with their profiles on other job boards to be sure they are who they say they are. And if somebody requires a bank account or credit card—run away fast.

As a fail-safe, people should check the website—or call—the company where they hope to work to see if the posted job is real. That’s how Mr. Ball learned that Civis was an employment-scam target: His human-resources department got droves of phone

inquiries about a position that wasn’t actually open.

AI and humans

The top employment sites use artificial intelligence and human teams to root out bad actors. Ada Yu, group product manager for careers at LinkedIn, says the company requires recruiters to verify that they are tied to the companies for whom they are hunting. Paul Wolfe, senior vice president of human resources at Indeed, says his site similarly uses AI and human readers to find bogus posts. Indeed has a “Report Job” button that lets users flag a suspicious posting.

Still, around 7% of all employment cons reported in 2020 to the BBB scam-tracker site, as noted in the organization’s 2020 report, originated on LinkedIn. “The majority of fake job postings are stopped before going live on our site,” says Ms. Yu, “but we don’t always get it right, and whenever we find fake posts, we work to remove them quickly.”

Nearly one-third of the fake postings began on Indeed, which is where Ms. Magno was duped. “My rule of thumb is, if anything seems too good to be true, it probably is,” says Mr. Wolfe. An Indeed spokeswoman added that, with some 250 million unique monthly users world-wide and around 10 jobs posted per second, there are bound to

be some bad guys slipping through. It is a constant game of Whac-A-Mole, she says.

The best way to avoid a scam, experts say, is to slow down. “About one-third of job hunters feel financial pressure, which makes them a little vulnerable,” says Ms. Pollak of ZipRecruiter. “But no legitimate job will require you to spend your own money before getting a paycheck.”

LinkedIn’s Ms. Yu says it’s very rare to get an offer or a request for personal information after just one interview—as sometimes happens with the scams. For instance, filling out a direct-deposit bank form after one interview isn’t the norm.

Ms. Magno wishes that she had taken the time to notice that some of the contact

information seemed “strange” and the punctuation and grammar were “off”—and especially wishes that she had quit communicating as soon as she was asked to spend her own money. “It was around the holidays and they were very convincing,” says Ms. Magno, who has since found steady work as a fiction writer for videogames. “I should have known better. But they were so good. Looking back, I’m actually pretty impressed with their scam.”

Ms. Mitchell is a writer in Chicago. She can be reached at reports@wsj.com.

Copyright ©2021 Dow Jones & Company, Inc.
All Rights Reserved.

87990cbe856818d5eddac44c7b1cdeb8

Appeared in the September 9, 2021, print edition as ‘That Great Job Offer? It May Be a Scam.’