

Online Scammers Prey on the Jobless

New York Times - August 6, 2009 - When Claude Vera responded to the customer-service job opening he saw on the online-classified site Geebo.com back in February, it seemed like one of a hundred small acts that might get him back to work. Most of his e-mail messages to prospective employers were going unanswered, so he was relieved when Penguin Express Inc. replied the next day with a work-from-home job.

To help him get a home office started, Penguin sent him money orders so he could buy, via money wire, the requisite laptop and other equipment from several different people. Mr. Vera, of Jamaica, New York, deposited nine United States Postal Service money orders into his Chase bank account and wired a total of nearly \$8,000 to the various vendors. But he never received a laptop or anything else, and the money orders turned out to be already cashed or counterfeit. The scam consumed Mr. Vera's tax refund and put him in the red by \$6,700 to Chase, which sent his case to a collection agent.

"Looking back at the whole thing I was very, very naïve, but I needed a job so bad," he says. "I'm behind in everything. I'm behind in my rent. I'm behind in all the bills I'm responsible for. It has wiped me out financially."

With unemployment high and rising, more people are streaming onto the Web in search of jobs, but running into costly scams. Like job seekers, criminals are after moneymaking opportunities online. And they're setting increasingly sophisticated traps to prey on the desperation of the jobless, whose guards are down amid eroding savings, swelling debts and calamities like foreclosure and bankruptcy. Victims can ill afford another financial setback.

"If you are a con artist, having more people out of work to deal with increases your odds of finding a victim," says Pam Dixon, executive director of the World Privacy Forum. "They are thriving right now. If business weren't good for the scammers, we wouldn't be getting so many complaints."

Spam filters provide some protection, and job boards work hard to remove bogus offers from large pools of legitimate offers. But none of the technology is foolproof. Job seekers have to keep their wits about them, no matter how much they need a job.

"The bottom line is if anything seems weird, just don't apply," says Tabatha Marshall, founder of PhishBucket.org, a non-profit that tracks online job scams and estimates they're up a third from a year ago. "You're going to take yourself down a road where you could lose money or time."

(continued)

Online Scammers Prey on the Jobless

Here are some of the more common scams and tips for avoiding them:

Common Frauds

HELP FOR A FEE

Watch out for fake recruiters and charlatans who promise to train you for a lucrative new career. A well-known scam of the latter type is Google Treasure Chest, which offers people a cheap DVD that will teach them how to prosper placing Google ads.

But in the small print of the buyer's agreement is notice of a \$72.21 monthly charge. Stopping the charges proves difficult; some people claim to have gotten relief only by changing their credit card numbers. Google Treasure Chest did not reply to requests for comment.

FISHING FOR IDENTITY DATA

Ads for attractive white-collar jobs can be, in fact, sophisticated fraud schemes.

Applicants may be steered to an authentic looking corporate Web site, where they are asked to type personal information into a fake human resources department Web form. Sometimes scammers go to great lengths, staging phone interviews or sometimes even conference calls with multiple people in an effort to appear legitimate. The goal? To talk people into handing over Social Security and bank account numbers.

WORK FROM HOME

Proliferating recently are fake "Mystery Shopper" positions evaluating the services of companies, especially money-wiring services. Victims are typically asked to deposit a check for several thousand dollars into their bank account, immediately use a bit of the money to shop at big-box stores and wire the rest via a service like Western Union or MoneyGram.

Of course, the check is counterfeit, leaving victims out any money they wired and opening them to criminal prosecution for passing a bad check.

MONEY-MULE AND RESHIPPER

These are some of the most dangerous schemes, since they can turn people, often unwittingly, into accomplices of international crime rings. More sophisticated than the now-familiar Nigerian e-mail messages, money mules are recruited by purported international companies looking for "receiving payment agents" who will accept payments into their bank account from "customers" (identity fraud victims) and wire the money to their "employer" (criminals).

Online Scammers Prey on the Jobless

Some are told to keep 10 percent, but many are promised payment by direct deposit, which, of course, never comes.

Reshipper scams start with international shipping companies looking for “logistics managers” to receive packages of laptops, iPods and cameras, bought with stolen credit cards, and send them on to a foreign country. Again, direct-deposit payment never comes.

How to Protect Yourself

BE SKEPTICAL

Red flags include offers using poor grammar and spelling and that come from e-mail addresses that don't match the name of the company. Real companies use polished language, emphasize a job's duties and use corporate e-mail addresses, not Yahoo or Gmail accounts.

DO YOUR HOMEWORK

Research the company. Do they have a professional Web site with lots of content, a list of executives' names and a phone number where you can reach a human being?

Often a simple Google search will be enough to spot trouble. There are scads of warnings from people who believe they were cheated by Google Treasure Chest, for instance. You can also check companies' reputations with the Better Business Bureau and look for complaints on Web sites like Complaintsboard.com and PhishBucket.org.

KEEP IT PRIVATE

Limit the personal information you give online. This starts with your résumé: Don't include any information you wouldn't want broadcast to the world, which is exactly what you're doing. Avoid providing your home address, a key bit of information for perpetrators of identity fraud; most real employers are happy with a general geographic location, like Greater New York City region. Unless you're signing an employment agreement, keep your Social Security number to yourself.

SPECIALIZE YOUR SEARCH

“If you are in a particular sector or profession, go to the niche site first,” Ms. Dixon says. Scammers want the volume provided by big sites. Moreover, niche sites often filter job posts by hand and tend to be intimately familiar with the companies posting them, making it easier for them to spot fakes. Look for industry-specific job boards or professional groups with online listings.

Online Scammers Prey on the Jobless

GET TO KNOW THE COMPANY

During the hiring process, both parties should be looking for a good fit. Craigslist's chief executive, Jim Buckmaster, says job seekers on his site should, as general rule, "deal with only local businesses you can meet face to face."

Mr. Buckmaster says Craigslist's system captures the large majority of scams before they reach the site, but "It's virtually impossible to keep every scam from traversing an Internet site that 50 million people are using each month."

GO LOW TECH

Most people get jobs through local want ads, professional associations, job-search agencies, temp agencies and their personal networks of colleagues, friends and family.

"The old-fashioned way is still sometimes the best way," says Linda Foley, a founder of the consumer advocacy Identity Theft Resource Center.

(End)