ARE YOU THE NEXT VICTIM?

BE ALERT, BE VIGILANT TO BE SAFE FROM SCAMS

BY TINA BERRES FILIPSKI

IN LATE JANUARY, LISA PARKE, owner of Advertising Specialties, LLC (UPIC: A330798) in Lexington, Kentucky, was busy with a client when she received a phone call from a woman named Valerie. The woman wanted to collect the $100 she said she earned from a job listed by Advertising Specialties on Craigslist. The problem was that Parke had not posted a job. Suddenly both women realized they were part of a scam.

Unfortunately, scams are nothing new and, as technology has become more ever-present in our daily lives, opportunities for criminals looking to pull a fast one have become more pervasive and more elaborate.

In Parke's case, the scammers posted a listing on Craigslist offering an easy $100 to anyone willing to go to a local mail store, sign for two boxes shipped there, re-label them and ship them to a Las Vegas address. Valerie bit.

She was told to pretend to be Parke's secretary and she completed the deed. When she didn't receive her $100 as promised, she looked up the phone number for Advertising Specialties and made the phone call to Parke that revealed the scam.

Parke immediately called police who investigated and found out the scammers had gone to the Kentucky Secretary of State website, paid a $10 filing fee and changed Parke's company address to the P.O. box. Then they opened a Verizon account with 15 phones listed under Parke's name. Three days later the perpetrators went back to the state website, paid another $10 filing fee and reversed the address

change to try to avoid detection. It was also discovered that the two boxes shipped to the mail store contained cell phones and cases. Although the motive remains unknown, police think Parke was used as a middleman for tracking and Parke guesses this was a trial run. If the scam had not been detected, she thinks future shipments could have contained drugs.

Identity theft is one of the fastest-growing crimes with 19 people falling victim every minute, according to credit reporting agency TransUnion. Parke faults the state's website for not having password protection. "We are living in a world of identity theft and there's no password protection on the Secretary of State's website," Parke says in dismay. "They are just putting our information out on a silver platter as if to say, 'Change anything you want for just $10!'"

Although police have kept the post office box open in case the scammers decide to send more packages, Parke is hopeful that her involvement is over. While she was fortunate not to have incurred any material losses, she is working to clear her name on a Verizon bill for $4,051 for the 15 phone lines, despite her notification to the company that a scam was in the works.

Her mission at this point is to alert other small-business owners to check their state's Secretary of State website to ensure their information is password-protected and to watch for suspicious activity. Parke is proud of her efforts to effect some change. As a result of her actions, the state now emails business owners if any action is taken on the site regarding their company information. She has also been told that late this summer the state will add password protection to its website.

Other Crimes To Watch For

Identity theft is just one type of a growing list of white collar crimes to which businesses can fall victim. Have you seen this email or one like it?

> *Hi,*
> *We will like to make a quote request on below items*
> *a) 2500pcs 4GB USB FLASH DRIVE*
> *b) 2500pcs 2gb micro sd card with adapter*
> *c) 2000pcs 8GB usb flash drive*
>
> *Regards*
> *Matt*
> *Purchasing manager*
> *delta created*
> *deltacreated@gmail.com*

This is an actual email that popped into my PPAI inbox as I was preparing to write this article.

"A lot of email scams are easy to spot," says Allison Schaffer, CAS, formerly the director of sales and marketing for technology products supplier Pingline and now a regional sales rep for TK Cups-Sorgs. "Scammers are typically looking for four or eight gig drives, and for external hard drives. Ninety to 95 percent of the emails are in broken English, may be addressed to Sir or Madam, have a lot of grammar mistakes and misspellings, and the emails often are from a gmail account."

18 Ways To Avoid Scams

1. Be alert to anything out of the ordinary. Lisa Parke says she should have become suspicious when she received several business calls asking for someone named Linda. Linda was the contact name given in the Craigslist ad.
2. Make sure your state's Secretary of State website is password protected. Companies located in Kentucky can call 502-564-3490 to ensure their email address is on file for activity alerts.
3. Be vigilant in checking your credit reports as often as possible and note any unfamiliar activity.
4. Check your personal credit card statements regularly for unauthorized charges.
5. When setting up a new customer, ascertain that the card holder name matches the name to whom the products are being shipped.
6. When shipping offshore, be wary of a shipping address that is an individual's home.
7. Research the address on Google Maps, which often provides snapshots of what a building looks like. Sometimes this step can help filter out fraudulent orders.
8. Make sure the address and phone number on the order match the information on the company's website.
9. Scammers almost always pay by credit card. When you establish open credit for an unfamiliar company, look it up in Dun & Bradstreet.
10. Double check the "Bill To" name on the order. Ascertain the credit card is not stolen.
11. Google the name of the company and call it to make sure it's genuine.
12. Be wary if you get an order from an unknown customer for promotional products that are normally decorated. Products with a high retail value such as undecorated t-shirts, USBs and other electronics are the products most often ordered in scams.
13. Be alert to emails with poor grammar and frequent misspellings. Business professionals likely have a better way of phrasing a request for pricing.
14. If the email address is a "generic" domain (Hotmail.com; google.com; msn.com), check out the order thoroughly.
15. Use caution if the requester offers to pay immediately by credit card or requests immediate shipment. This is often a red flag of a scam.
16. Be alert if the order "ship to" address does not match the "bill to" address.
17. Know the person or company to whom you are selling. If you don't know them, find someone you know who does.
18. Don't go for the easy buck. Chances are you won't collect.

Unfortunately, Schaffer is familiar with a number of situations where distributors fulfilled bogus orders and did not get paid. "The emails have been coming around for years but are more common now—and more frequent," she says. "There are distributors who look at these emails and hesitate—with good reason. These emails are sent directly to suppliers and distributors—100 people at a time—hoping someone will bite. Fortunately, as a supplier, I do my due diligence to help my customers. If you are unsure, send the email to a supplier. Most suppliers who deal with tech products have probably gotten the email, too."

She recommends distributors also do their due diligence by researching the email sender. If the email has an address for shipment, look it up on Google Maps and see what exists at that address. Call the phone number—if your call goes to a nondescript voicemail, that's your first clue the order may not be legitimate. "I got an order by email with a ship-to address in Hackensack, New Jersey—but they spelled it wrong," says Schaffer, a Jersey native. "The website was nondescript, so I Googled it and found the company and its address matched the one in the email but the phone number wasn't working. I Googled the address, called the company and asked for the person in the email—there was no one there by that name," she says. "Don't take an order just because it looks good on paper. You may be out thousands of dollars."

HALO Branded Solutions (UPIC: HBS) is one distributor on high alert to these types of scams and trains its employees and account executives to know what to look for. "We were lucky to catch on to the scams fairly quickly several years ago," says Terry McGuire, CAS, executive vice president. He adds that the company started to notice a pattern in 2011. "We had challenges with a couple of orders and a couple that actually went through, but the person whose card was charged challenged the charges. We realized it was creating vulnerabilities with our credit card merchant services agreement." The company looked at the pattern of fraudulent orders and sent a notice to its sales force to point out the characteristics of these fraudulent orders and has since eliminated them. HALO's

How An Apparel Supplier Filters Go From No-Go

Kevin Shea, manager of the inside sales team at SanMar (UPIC: SNMR), shares his company's best practices to avoid order scams.

Is there an email scam situation you can recall? What happened and when did you discover the order was fraudulent?

Shea: SanMar only sells to authorized customers, so we were unaware that they were involved in a scam until they let us know they had trouble with payments from some of their end users. Our customers mentioned that they had accepted and shipped orders, but were unable to collect payment once the products had been delivered because the end user supplied stolen credit card information. After a few of those calls, we realized that there might be a connection.

What characteristics do these orders have in common?

Shea: We looked into the orders that our customers flagged as part of a scam and noticed some commonalities between the reports. The orders were generally for large quantities of t-shirts (all in one or two sizes and in one or two colors) and were shipped to common addresses and had common names associated with them.

What steps is SanMar taking to prevent scams?

Shea: If our inside sales team notices a suspicious address or name we make it a priority to contact the customer that placed the order and share our concerns. We also have a dedicated inside sales team member who monitors the names and ship-to addresses that had been identified as suspicious by our customers. Scammers are always changing their tactics, but we do our best to provide our customers with the latest information we have if we think their order might be part of a scam.

How is SanMar advising its customers?

Shea: We believe that it is a best practice to only accept orders from known or verified end users. We advise our customers to trust their instincts and if something seems odd about an order, ask more questions to verify the legitimacy of the customer and the order. A quick internet search can also be useful if other businesses have reported problems with certain addresses or end users.

Similar to what we recommend to our customers, we train our staff to pay attention to any orders that are strange or inconsistent with the typical customer order. If we discover an unusual order that seems like it may be part of scam or if we recognize that the ship-to address is one of the addresses flagged by customers, we share that information with our customers so that they can make the best decision.

> *There are people who make it their mission in life to take advantage of people who aren't paying attention. We are always looking for what could be the next thing. The difference between now and four years ago is the ability for people to get large numbers of valid credit cards.*
>
> —DAWN OLDS, HALO SENIOR VICE PRESIDENT OF OPERATIONS

internal accounts receivables area also adopted changes aimed at flagging questionable orders.

McGuire points out that the issue is more than about getting paid. "Just because the credit card goes through does not mean there won't be repercussions for distributors," he says. "You risk the ability to work with the credit card companies in the future if you process payment that you suspect is not legitimate." Dawn Olds, HALO senior vice president of operations, adds, "If the customer refuses the charge and they show they didn't authorize the charge, you will be charged back, and too many charge-backs will raise your rate with the credit card companies. Eventually, you will lose your ability to charge any customer cards."

She also adds that if companies routinely accept bad cards, the news can quickly spread on social media and hurt the company's reputation.

HALO's stringent procedures have paid off, but companies can't let down their guard. "There are people who make it their mission in life to take advantage of people who aren't paying attention," says Olds. "We are always looking for what could be the next thing."

"The difference between now and four years ago is the ability for people to get large numbers of valid credit cards," adds McGuire.

McGuire had a recent personal experience where the business credit card he uses for international travel was stolen while in China. A few weeks later, he noticed a $6,000 charge on his statement from a printing company located about an hour away. "It was for a shipment of printed materials to India," he says. He called the printing company and asked who authorized the charge. "They said, 'We thought it was strange that someone with that accent was named Terry McGuire but we processed the card anyway,'" says McGuire, with a sigh. "The key thing is to have a written protocol on how to identify these types of scams and how to deal with it within your organization and distribute the information throughout your organization. You can't assume that it's as obvious to everyone else as it is to you." PPB

Tina Berres Filipski is editor of *PPB*.