Technology, sour economy breed, feed Internet scams

May 6 2009, By David Flick

Ute Schnetzinger thought the bride was demanding. Only later did the Richardson, Texas, florist learn she was bogus.

In a series of lengthy e-mails that began last Thanksgiving and persisted into the new year, the "bride" -- claiming to be from Manchester, England -- placed a detailed order with Schnetzinger, co-owner of Gunter's Greenhouse, to help decorate her spring wedding in the Dallas area.

The correspondent was amiable, even chatty, but she also chided Schnetzinger for not responding quickly enough, seemed unusually curious about her family and insisted that the florist pay a musical band out of a $3,600 check she had accidentally sent in as overpayment.

The check was a trap. Schnetzinger deposited it, thought twice, then went to a bank official, who recognized it immediately as fake.

"Whoever did this did their homework. Everything was so detailed, and she seemed to know so much about us," Schnetzinger said. "Life is getting more complicated, and you have to warn people about everything."

Scams are as old as history. But Internet fraud, which already had been accelerating with each technological innovation, has been given a new opportunity with the economic downturn.

John Kane has called it a "perfect storm."

Kane is the author of the Internet Crime Complaint Center's annual report on computer crime. The center, in Fairmont, W.Va., is a combined effort of the FBI and the National White Collar Crime Center.

"When you have what we've been seeing for the past few years, which is the rise of various types of increasingly sophisticated technology, combined with the bad economic climate, it really creates a very difficult situation," he said.

The 2008 report found that scam reports to the Internet crime center had increased 33 percent over the previous year to a record 275,285 complaints. And figures for the first three months of this year are running about double those in the months covered by the report, a center spokesman said.

Another agency -- the Federal Trade Commission -- said it compiled 1.2 million complaints last year from a variety of law enforcement sources, up from 230,600 in 2000.

The popularity of social networking sites has been a boom for scammers, Kane said.

"They can infiltrate your Facebook account and send e-mails to your friends, saying, 'I've been in a skiing accident,' and they ask for money," he said. "If you think it's from a friend, you might consider sending something."

Fraudulent e-mails looking like authentic messages from a person's bank can be sent to cellphones.

Scammers can also break into sites of professional or social

organizations, then use the information to target victims, who in turn think the messages have validity because the sender seems familiar with their job or lifestyle.

"The Internet that has made our lives easier has made scammers' lives easier too," Kane said.

The advances in technology, he said, would probably have increased the number of scams in any case, but the sudden downturn in the economy made things worse -- in two respects.

"You have tech-savvy individuals who are out of work and turn to scamming as a means of income," Kane said. "They do this for a living, and they do it very well."

But more obviously, the tight times have made some people desperate for money, and more susceptible to scams.

Among them was Sylvia Rodriguez, a Plano, Texas, loan office employee, who was struggling to make house payments last May when she got an official-looking offer inviting her to apply for a government grant.

After pursuing the offer, she was told that she could receive $3,000, but first she need to wire the "agency" $150 to cover transfer of the money. When she did so and the grant didn't materialize, she was told she could increase her grant application to $5,000 -- if she wired more money.

Over the next year, the back and forth continued. In order to cover the money transfers, she stopped paying her phone bill, fell further behind on house payments and borrowed from friends. Over the course of the year, she sent the scammers about $3,000.

Although the arrangement sounded increasingly fishy, Rodriguez said, she was afraid to tell her daughters, one of whom was a paralegal.

"I think if I told them, they would have looked into it, but I was too embarrassed to tell them about losing all that money," she said.

During a trip to a grocery last week, she mentioned her problem to a store employee, who advised her to go to the Better Business Bureau.

The BBB of Metropolitan Dallas gets such complaints all the time, said Jeannette Kopko, the local senior vice president. And these days, her staff may be more sympathetic than ever. The organization was itself recently victimized.

"People received a notice that appeared to be from us and had our logo telling companies that they were being investigated," Kopko said. "It would include a note that said 'download here' to see the complaint."

When the business owners clicked on the icon, it would download a program that could harvest the information on their computers.

The common assumption is that scams are primarily aimed at the elderly, but statistics don't necessarily back that up.

According to a Federal Trade Commission report published in February, 40- to 49-year-olds accounted for the largest number of complaints -- 26 percent of the total. Complainants 60 to 69 years old and those older than 70 accounted for about 4 percent each.

Identity theft victims tended to be even younger. The largest group reporting complaints were 20- to 29-year-olds.

Nor are all the victims necessarily unemployed or poorly educated.

Kopko said an accountant told her one of his clients received a classic "Nigerian scheme" e-mail in which someone purporting to be a relative of an African official asked for monetary help in obtaining a large sum of money.

"The accountant told him that there's a 99.9 percent chance this is a scam, and the client replied, 'What if it isn't'?" Kopko said. "It's a lottery mentality. A lot of people think, 'Well, maybe this is my lucky day.'"

While the FTC report found that more than half of modern scams involve the Internet, some scammers are apparently still traditionalists.

Amanda McMurrey, a spokeswoman for the U.S. Postal Inspection Service's Fort Worth division, said just under a quarter-million fake checks were seized from April 2007 to June 2008 at Dallas/Fort Worth International Airport. If they had been valid, the checks would have equaled $1.15 billion.

"I think whenever the economy turns down, people are always looking to make money," she said. "Unfortunately, it is part of our psyche as Americans to want to make a lot of money quickly with very little effort."

But if the Internet has created better tools and more opportunity for crooks, McMurrey said, it also makes instant information available to help protect consumers.

The best protection, she said, doesn't require technological savvy.

"A lot of people could avoid trouble," McMurrey said, "if they would listen to the little voice in their head that tells them something is too good to be true."

___

TIPS TO AVOID SCAMS

Warning signs and tips that might help you avoid being a scam victim:

GENERAL TIPS

• If it looks too good to be true, it probably is.

• Fact checking, good judgment and a healthy dose of skepticism are the best defenses.

• Use common sense: There is no legitimate reason anyone would give you a check or money order and ask you to wire money in return.

• If you have a question about a company, contact the Better Business Bureau.

• Rational people can make irrational decisions when under stress. If you are in financial trouble, recognize your vulnerability and think twice before you get involved in a suspicious venture.

MONEY-ORDER SCHEME

• Be skeptical of anyone asking you to wire money to overseas bank accounts or to cash money orders or checks on their behalf.

• Familiarize yourself with postal money-order security features.

• Never wire funds to anyone unless you're sure the money order or check they gave you was cleared by your bank and the funds released.

• Resist pressure to "act now." If the offer is good now, it should be good when the check or money order clears.

PURCHASING MERCHANDISE

• Try to obtain a physical address rather than merely a post office box and a phone number. Call the seller to see if the number is working.

• E-mail the company to see if it has an active e-mail address. Be wary of sellers who use free e-mail services where a credit card wasn't required to open the account.

• Check out other Web sites regarding this person/company.

IDENTITY THEFT

• Never give your Social Security number -- or personal information of any kind -- over the telephone or online unless you initiate the contact.

• Check your credit reports. Look for telltale signs such as an address change you didn't make.

• Monitor your bank account statements frequently for suspicious activity.

• Shred or tear up unwanted documents that contain personal information.

BOGUS CHARITY SCAM

• Most states require charities to register and file annual reports showing how they use donations.

• Many unsolicited e-mail messages are fraudulent.

• Some crooks try to fool people by using names that are similar to those of well-known charities.

• Be wary of requests to support police or firefighters. Scammers often use the popularity of these occupations to run fake charities.

• Be cautious when there are natural or other disasters. Fraudulent charities take advantage of people who want to help the victims.

WORK-AT-HOME FRAUD

• Don't get involved with an employer that can't make its business model clear to you or one that's willing to hire you without even a phone interview.

• Do your own research on any employer that makes you feel uneasy.

NIGERIAN OR "419" FRAUD

• If you receive a letter from Nigeria or any other foreign country asking you to send personal or banking information, do not reply.

• Be skeptical of individuals representing themselves as foreign government officials asking for your help in placing large sums of money in overseas bank accounts.

• Do not believe the promise of large sums of money for your cooperation.

SWEEPSTAKES/PRIZE SCAMS

• You should never have to pay to enter a sweepstakes. That includes paying shipping fees or buying a product to receive your "prize."

• If you can't understand what you must do to be eligible, think twice about responding.

• Make sure the prizes are desirable and worth the effort.

• No legitimate prize company asks for personal information to declare you a winner.

Source: Dallas Morning News research

___