New scam involves PayPal and Western Union

By Woody Leonhard

There's a new variation on the old "Nigerian" or "419" scam, one that invokes the names of PayPal, Western Union, and the FBI — and the scammers are raking in billions.

Let me introduce you to the way these scum operate — and show you a few tricks that may keep you from adding to their booty.

"Greetings, I am writing this letter to you in good faith and I hope my contact with you will transpire into a mutual relationship now and forever. I am Mrs. Omigod Mugambi, wife of the late General Rufus Mugambi, former Director of Mines for the Dufus Diamond Dust Co. Ltd., of Central Eastern Lower Leone …"

I'm sure you're smart enough to pass over e-mail like that — at least, I hope so. It's an obvious setup for the classic 419 scam — also known as the Russian scam, the Detroit/Buffalo scam, and, of course, the Nigerian Letter, as described in a Wikipedia page. (The 419 moniker is derived from the Nigerian Criminal Code, Chapter 38, Article 419: "Obtaining property by false pretences; cheating.")

Recently I bumped into a more sophisticated version of the same kind of scam and tried to trace it all the way back to its source. I'll take you through the scam's stages and show you some of its wrinkles. Plus I'll whine about the way big companies such as PayPal and Western Union are letting us down, and I'll talk about how I rode the paperless trail to its roots. You may be able to, too.

There's a reason why everybody gets so much 419-scam e-mail. It's a huge business. The 419 Coalition says that, as early as 1996, 419 scams netted U.S. $5 billion. The subsequent rise of the Internet and e-mail has only increased the opportunities for this type of fraud. (While Nigeria does harbor its share of 419 scams, perpetrators can be found in all corners of the globe, including the U.S. But, as you'll see shortly, there are significant advantages to working out of small countries.

New wrinkle on an old ploy — the PayPal scam

It all starts when you place an online ad.

It doesn't really matter what you're selling, as long as it's physically large and valuable. It doesn't matter where you advertise — I've seen reports of this ploy being played on Craigslist advertisers and other major online sites.

I first found out about this PayPal 419 scam when a handful of advertisers in my local newspaper all got hit within just a few weeks of each other.

One of the intended victims contacted me the minute he received the first solicitation. He agreed to let me step in and act on his behalf. Here's what happened.

The scammer, PaulW (modified by this author), sends me this message from a Gmail address: "I will like to know if this item is still available for sale?" I write back and say, yes, it is, and he'd be most welcome to come and take a look at it.

PaulW writes: "Thanks for the response, how long has your friend owned this item? let me know the price in USD? I am OK with the item it looks like new in the photos I am from Liverpool UK, i am sorry i will not be able to come for the viewing, i will arrange for the pickup after payment has been made, all documentation will be done by the shipper, so you don't have to worry about that. Thanks"

Three key points: The scammer is using a Gmail address, which is nearly impossible to trace without a court order; he claims to be out of the country; and he claims that he has a shipper who will pick up the item. The plot thickens.

I write back and say that the item's practically new, I give him a price, but I express concern about the shipper.

PaulW replies: "My shipper will be coming from UK for the pickup, and pls tell your friend to prepare all the export documentations for the pickup. I'm quite satisfied with the condition and price. I will be paying the PayPal charges from my account and i will be paying directly into your PayPal account without any delay, and i hope you have a PayPal account."

I respond, giving him a dormant PayPal account and my "address" (which is, in fact, my local police station).

He quickly writes back: "I have just completed the Payment and i am sure you have received the confirmation from PayPal regarding the Payment. You can check your paypal e-mail for confirmation of payment.a total of 25,982usd was sent, 24,728usd for the item and the extra 1,200usd for my shipper's charges,which you will be sending to the address below via western union."

(I'll call the shipper William C. I've deleted the address because it actually exists in Devon, England. A different person, being scammed at about the same time, was also instructed to send money to the same Devon drop.)

Note the ploy here: I'm supposed to immediately send $1,200 to the shipper via Western Union. Of course, no PayPal payment to cover both the purchase and the shipping was ever sent.

"You should send the money soon so that the Pick Up would be scheduled and you would know when the Pick Up would commence, make sure you're home. I advice you to check both your inbox or junk/spam folder for the payment confirmation message."

I then receive a message claiming to be from "Service-Intl.PayPal.Com":

"The Transaction will appear as soon as the western union information is received from you,we have to follow this procedure due to some security reason … the Money was sent through the Service Option Secure Payment so that the transaction can be protected with adequate security measures for you to be able to receive your money. The Shipping Company only accept payment through Western Union You have nothing to doubt about, You are safe and secured doing this transaction and your account will be credited immediately the western union receipt of *1,200USD* is received from you."

From that point on, it was hard to keep a straight face — you'd think the scammers would put some effort into writing business-quality, standard-English sentences (or pay someone to edit them). But "PaulW" and "Service-Intl.PayPal" got progressively more strident when I asked questions about the PayPal Service Option Secure Payment method (which doesn't exist). The tone turned downright abusive; I eventually

received a message from a different e-mail address, **Service[at]Intl.PayPal[dot com],** (address modified by this author) with the FBI logo at the top (shown in Figure 1).

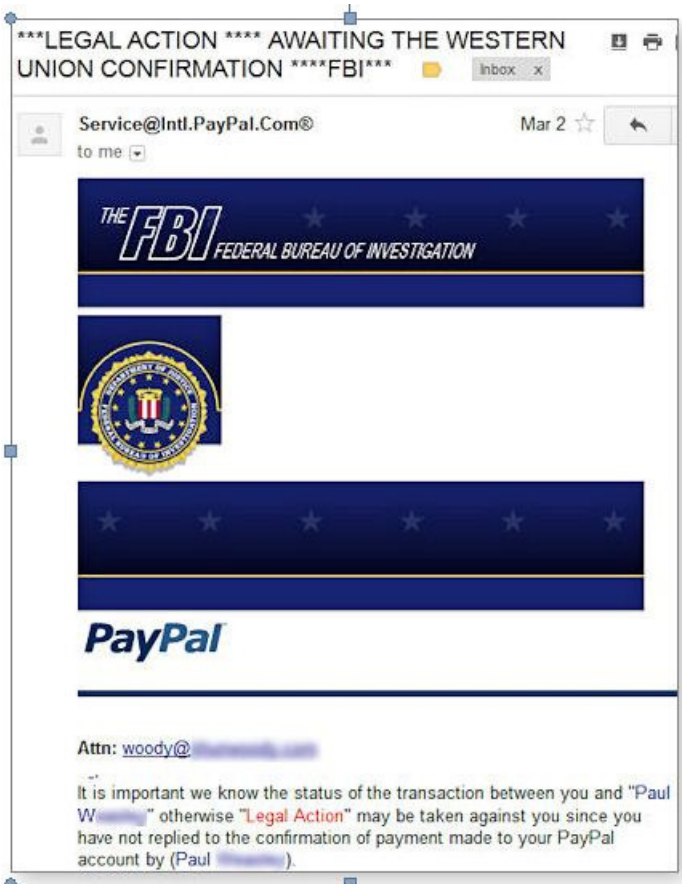

Figure 1. The scammer's threat included a "Federal Bureau of Investigation" letterhead.

The e-mail threatened to take legal action against me: "We use proprietary technology and constantly innovate to help ensure your transactions are safe. In addition, PayPal has over 20,000 staffs worldwide dedicated to keeping PayPal accounts safe, and stopping online criminals. And we work with Internet Service Providers (ISPs) worldwide to shut off fraudulent websites as soon as possible."

I exchanged several dozen e-mails, trying to get the scammers to reveal themselves — to no avail. Eventually, they stopped trying. It's possible they were tipped off after my calls to their ISP, or they simply moved on to easier targets.

Tips that the offer was not on the up-and-up

I knew this was a scam from the beginning. Several people in my area sent complaints to the local newspaper, describing virtually identical ploys — similar messages but with different e-mail addresses. (That was mistake number one.)

Although PaulW's message wasn't very convincing, he did use a Gmail account, which (as noted earlier) is essentially impossible to trace. I Googled PaulW's original e-mail address to see whether it was linked to other scams, but I didn't get any hits. So that part of the subterfuge worked.

But the rest of the scam was sloppy. The initial "PayPal" message had a return address of **Service-Intl.PayPal[dot com] | notification.verification[at]consultant [dot com].** Search **[at]consultant[dot com]** through Google, and you find references to scams. Go to **www.consultant[dot com],** and you'll see one of those generic index sites. When I looked at it, there was just one, bogus, online advertisement.

Most of the time, when the scammers sent e-mail from "PayPal," they used a virtual private network (VPN) to make it look like the messages originated in the U.S. But on three separate occasions, they forgot to turn on VPN. Using a very simple technique, I traced all three messages back to one specific Internet service provider in Lagos, Nigeria (see Figure 2).

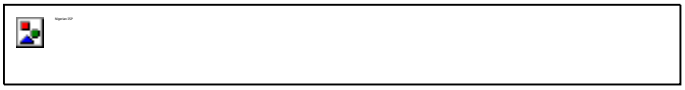

Figure 2. Three of the messages originated with the same ISP in Lagos, Nigeria.

Here's how to find the originating ISP of an e-mail:

- In Gmail, click the down arrow next to the right of the message header (next to the Reply button) and choose **Show original.** That shows you the entire message, including the full header information (the message routing information at the beginning of the message, which is normally hidden).
- Copy the entire header and go to the ipTRACKERonline header-analysis page.
- Paste the header info into the **Email header analysis** input box and press the Submit button.
- After ipTRACKERonline reloads the page, scroll down to the **Email header analysis report** box. There you'll see where the message has been and — most of the time — where it originated.

For more on tracking down e-mail origins, see Susan Bradley's Nov. 10, 2011, story, "Find out where that e-mail really came from."

What can be done to nail the scammers

So I now had three scam messages with identified IP addresses, the name of a large Internet service provider in Nigeria, and a compelling case for both PayPal (to defend its name) and Western Union (which was being used as a drop) to follow up.

Here's what happened next.

I went to the Western Union site and tried — nearly in vain — to find a security-related, customer-service e-mail address — someone I could talk to about WilliamC in Devon, England, and his apparent use (either knowingly or unwittingly) as a money-laundering mule for these scammers.

The Western Union site has acres and acres of warnings, cautions, and lip service about fraud, rip-offs, and cons. It has links to every single consumer protection agency in the U.S. It also has a customer-service 800 number, but it's hard to put an e-mail header into a phone conversation. In the end, Western Union was of no real help. (We eventually found a fraud-reporting e-mail address listed in small type at the bottom of the company's Phone and Mail Support page. — Ed.)

Moving from Western Union to PayPal was like night to day. PayPal displays its scam-reporting e-mail address prominently in many of its fraud discussions. I sent a copy of the first scam e-mail to spoof@Paypal.com with an open header and soon received a polite response saying, "Thanks for forwarding that suspicious-looking e-mail. You're right — it was a phishing attempt, and we're working on stopping the fraud. By reporting the problem, you've made a difference!"

Except it wasn't a phishing attempt. It was a scam that used PayPal as a key prop in the setup. So I sent a copy of the second fraudulent e-mail, explaining that it's a 419 scam. I got back another nice letter that said, "Thanks for forwarding that suspicious-looking email. You're right — it was a phishing attempt, and we're working on stopping …." Yes, it appeared to be a form letter. I sent three messages to PayPal, and I don't think a human looked at any of them.

Next, I wrote to MTN Nigeria, the Internet service provider in Africa, and they did respond. But the upshot was disheartening: "All of our 3G network subscribers now sit behind a small number of IP addresses. This is done via a technology called Network Address Translation. In essence it means that one million subscribers may appear to the outside world as one subscriber, since they are all using the same IP address." It's akin to a massive home network.

No doubt MTN Nigeria could sift through their NAT logs and find out who was connected at precisely the right time. But tracing a specific e-mail back to an individual would be difficult — if not impossible. And it would probably require a court order. On the bright side, my complaint was forwarded to the police. (I'm not, however, holding my breath.)

The bottom line? From a technical aspect, there's little that can be done about these scams. No doubt, thousands of folks around the world are victims. The solution is to bring these scams into the light and to use common sense when transacting business with strangers via e-mail. Any transaction that seems a bit unusual should raise red flags.

That said, there's something to be said for baiting the bustards and making them waste time on someone who isn't going to fall for their tricks. The 419 Eater blog has some handy suggestions.

If you know ***anybody*** who posts ads online, forward this article to them — they just might thank you for saving their bacon.